PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-233795
(43)Date of publication of application : 22.08.2003

(51)Int.Cl. G06K 19/10
G06F 12/14
G06K 17/00
G09C 1/00
H04L 9/32

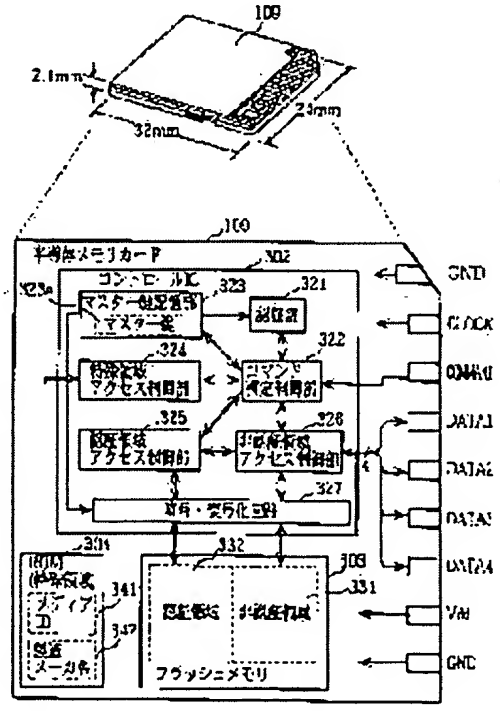
(21)Application number : 2002-346019
(22)Date of filing : 28.12.1999

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HIROTA TERUTO
TATEBAYASHI MAKOTO
YUGAWA YASUHEI
MINAMI MASANAO
KOZUKA MASAYUKI

(30)Priority
Priority number : 11119441 Priority date : 27.04.1999 Priority country : JP

(54) SEMICONDUCTOR MEMORY CARD AND READING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a semiconductor memory card, which can be used as a storage medium of digital literary works, and as a storage medium of general computer data (non-literary works) not requiring a protection of literary works.
SOLUTION: This card comprises a control IC 302, a flash memory 303, and a ROM 304. The ROM 304 holds a media ID 341 and the like unique to this card. The flash memory 303 has a certification area 332 allowing access for external equipment only when certification of the external equipment is succeeded, and a non-certification area 331 allowing access regardless of the certification results. The control IC 302 has control parts 325, 326 controlling access to the certification area 332 and the non-certification area 331 from the external equipment, a certification part 321 executing mutual certification to the external equipment and the like.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is a semi-conductor memory card removable on electronic equipment. Rewritable nonvolatile memory, The control circuit which controls access by said electronic equipment to the authentication field and the non-attesting field which are two storage regions where it was beforehand set in said nonvolatile memory, It has the area-size modification circuit which changes the area size of said authentication field and each of said non-attesting field. Said control circuit The non-attesting field access-control section which controls access by said electronic equipment to said non-attesting field, The authentication section which tries authentication of said electronic equipment in order to verify the justification of said electronic equipment, It has the authentication field access-control section which permits access by said electronic equipment to said authentication field only when said authentication section succeeds in authentication. Said authentication field and said non-attesting field It is assigned to each field obtained by carrying out the storage region where the fixed size in said nonvolatile memory continued for 2 minutes. Said area-size modification circuit The authentication field translation table showing correspondence with the logical address and the physical address in said authentication field, The non-attesting field translation table showing correspondence with the logical address and the physical address in said non-attesting field, It has the translation table modification section which changes said authentication field translation table and said authentication field translation table according to the instruction from said electronic equipment. Said authentication field access-control section Access by said electronic equipment is controlled based on said authentication field translation table. Said non-attesting field access-control section Access by said electronic equipment is controlled based on said non-attesting field translation table. Said authentication field and said non-attesting field It is assigned to the high field and the low field of the physical address obtained by carrying out the storage region of said fixed size for 2 minutes, respectively. Said non-attesting field translation table The logical address and a physical address are matched so that the ascending order of the logical address may turn into ascending order of a physical address. Said authentication field translation table The semi-conductor memory card characterized by matching the logical address and a physical address so that the ascending order of the logical address may turn into descending order of a physical address.
[Claim 2] It is the semi-conductor memory card according to claim 1 characterized by for said authentication section generating the key data reflecting the result of authentication, decoding said authentication field access-control section by the key data by which said authentication section generated the enciphered instruction which is sent from said electronic equipment, and controlling access to said authentication field according to the decoded instruction.
[Claim 3] Said authentication section is a semi-conductor memory card according to claim 2 characterized by generating said key data from the response data generated in order to prove the challenge data transmitted to said electronic equipment in order to perform mutual recognition of said electronic equipment and a challenge response mold and to verify the justification of said electronic equipment, and self justification.
[Claim 4] The enciphered instruction which is sent from said electronic equipment It consists of the tag

section which specifies the classification of access to said authentication field and which is not enciphered, and enciphered address part which pinpoints the field to access. Said authentication section The semi-conductor memory card according to claim 3 characterized by carrying out execution control of the access of the classification specified by the tag section of said instruction to the field which decodes the address part of said instruction and is pinpointed by the decoded address using said key data.

[Claim 5] It is the semi-conductor memory card according to claim 4 characterized by equipping said semi-conductor memory card with the discernment data store circuit which memorizes beforehand the discernment data of the proper which can specify self in distinction from the semi-conductor memory card of further others, for said authentication section performing mutual recognition using the discernment data stored in said discernment data store circuit, making it dependent on said discernment data, and generating said key data.

[Claim 6] Said semi-conductor memory card is a semi-conductor memory card according to claim 1 characterized by having the read-only memory circuit in which data were stored further beforehand.

[Claim 7] Said authentication field and said non-attesting field consist of a storage region which can be written for said electronic equipment, and a read-only storage region. Said control circuit has the random number generator which generates a random number whenever it accesses further for said electronic equipment writing data in said nonvolatile memory. Said authentication field access-control section and said non-attesting field access-control section The semi-conductor memory card according to claim 1 characterized by writing said random number in said read-only storage region matched with said encryption data while enciphering and writing said data in the storage region which can write [said] the obtained encryption data using said random number.

[Claim 8] Said control circuit is a semi-conductor memory card according to claim 1 characterized by having the code decode section which decrypts the data read from said authentication field and said non-attesting field while enciphering further the data which should be written in said authentication field and said non-attesting field.

[Claim 9] It is the semi-conductor memory card according to claim 1 characterized by for said nonvolatile memory being a flash memory and having the non-eliminated list read-out section which sends the information which said control circuit pinpoints the field which is not eliminated [which exists in said authentication field and said authentication field further according to the instruction from said electronic equipment], and shows the field to said electronic equipment.

[Claim 10] The user key storage section for said authentication section to require the user key which is the information on a proper of the user from the user who uses electronic equipment for authentication, and for said control circuit memorize said user key further, The identification information storage section for memorizing the identification information which can specify the electronic equipment which succeeded in authentication by said authentication section, If authentication by said authentication section is started, identification information will be acquired from the electronic equipment. The semi-conductor memory card according to claim 1 characterized by having the user key demand prohibition section in which the demand of the user key by said authentication section is forbidden when the identification information inspects whether it is already stored in said identification information storage section and is already stored in it.

[Claim 11] It is read-out equipment which reads the digital work stored in the semi-conductor memory card according to claim 1. Said semi-conductor memory card While the digital work is stored in the non-attesting field, the count which permits read-out of said digital work is beforehand stored in an authentication field. Said read-out equipment A decision means to judge whether the count stored in said authentication field is read, and read-out is permitted by the count in case the digital work stored in said non-attesting field is read, Read-out equipment characterized by having the playback means which subtracts said read count and is returned to said authentication field while reading said digital work from said non-attesting field, only when the permission is granted.

[Claim 12] It is read-out equipment which reads the digital work stored in the semi-conductor memory card according to claim 1, and is reproduced to an analog signal. Said semi-conductor memory card

While the digital work refreshable to an analog signal is stored in the non-attesting field The count which permits the digital output by said electronic equipment of said digital work is beforehand stored in an authentication field. Said read-out equipment A playback means to read the digital work stored in said non-attesting field, and to reproduce to an analog signal, Only when the permission is granted with a decision means to judge whether the count stored in said authentication field is read, and the digital output is permitted by the count, while outputting said digital work outside with a digital signal Read-out equipment characterized by having the digital output means which subtracts said read count and is returned to said authentication field.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the suitable semi-conductor memory card for protection of copyrights and read-out equipment of a digital work especially about the semi-conductor memory card and its read-out equipment for memorizing a digital work etc.
[0002]
[Description of the Prior Art] Digital works, such as a music content, come to be distributed by development of a multimedia network technique through communication networks, such as the Internet, in recent years, and it has become possible to touch the music in the world etc. at a house. For example, after downloading a music content with a personal computer (henceforth "PC"), music can be played and enjoyed by storing in the semi-conductor memory card with which PC was equipped if needed. Moreover, music can also be listened to with a walk by taking out from PC the semi-conductor memory card which did in this way and stored the music content, and equipping a pocket mold music regenerative apparatus. Such semi-conductor memory cards are non-volatiles, such as a flash memory, and are convenient small lightweight cards which contained the semiconductor memory of big storage capacity.
[0003] By the way, when memorizing a digital work to a semi-conductor memory card, in order to prevent an unjust copy, in such an electronic music distribution, it is necessary to use a key etc. and to encipher contents. Moreover, it is necessary to prevent from copying to other storages etc. depending on the file management software which standard attachment was carried out at PC etc. and has appeared on the market widely.
[0004] The policy which enables access to a semi-conductor memory card only by the software of dedication as an approach of preventing such an unjust copy can be considered. For example, when authentication between PC and a semi-conductor memory card is successful and it cannot succeed in the authentication since it supposes that access to a semi-conductor memory card is permitted and there is no software of dedication, the approach of supposing that access to a semi-conductor memory card is forbidden can be considered.
[0005]
[Problem(s) to be Solved by the Invention] However, in the software of dedication always being needed for PC accessing a semi-conductor memory card, it will become impossible to carry out the data exchange mutually freely through the unspecified user and unspecified semi-conductor memory card which do not own the software of such dedication. Therefore, the convenience that PC can be accessed by the file management software by which standard attachment is carried out is no longer acquired, without needing the convenience which the conventional semi-conductor memory cards, such as a flash plate ATA and CompactFlash (trademark), had, i.e., the software of dedication.
[0006] That is, although it is suitable as a storage of a digital work in that an accessible semi-conductor memory card has the function of protection of copyrights only by the software of dedication, since general-purpose use is difficult, there is a trouble that it cannot be used as an auxiliary storage unit in a

general computer system. Then, this invention is made in view of such a trouble, and aims at offering the semi-conductor memory card [using as a storage of a digital work is possible and] which can be used also as a storage of the common computer data (non-work) for which protection of copyrights is not needed, and its read-out equipment.

[0007]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the semi-conductor memory card concerning this invention It is a semi-conductor memory card removable on electronic equipment. Rewritable nonvolatile memory, The control circuit which controls access by said electronic equipment to the authentication field and the non-attesting field which are two storage regions where it was beforehand set in said nonvolatile memory, It has the area-size modification circuit which changes the area size of said authentication field and each of said non-attesting field. Said control circuit The non-attesting field access-control section which controls access by said electronic equipment to said non-attesting field, The authentication section which tries authentication of said electronic equipment in order to verify the justification of said electronic equipment, It has the authentication field access-control section which permits access by said electronic equipment to said authentication field only when said authentication section succeeds in authentication. Said authentication field and said non-attesting field It is assigned to each field obtained by carrying out the storage region where the fixed size in said nonvolatile memory continued for 2 minutes. Said area-size modification circuit The authentication field translation table showing correspondence with the logical address and the physical address in said authentication field, The non-attesting field translation table showing correspondence with the logical address and the physical address in said non-attesting field, It has the translation table modification section which changes said authentication field translation table and said authentication field translation table according to the instruction from said electronic equipment. Said authentication field access-control section Access by said electronic equipment is controlled based on said authentication field translation table. Said non-attesting field access-control section Access by said electronic equipment is controlled based on said non-attesting field translation table. Said authentication field and said non-attesting field It is assigned to the high field and the low field of the physical address obtained by carrying out the storage region of said fixed size for 2 minutes, respectively. Said non-attesting field translation table Said authentication field translation table is characterized by matching the logical address and a physical address so that the ascending order of the logical address may turn into ascending order of a physical address, and matching the logical address and a physical address so that the ascending order of the logical address may turn into descending order of a physical address.

[0008]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing. Drawing 1 is PC which downloads digital works, such as a music content, through a communication network, and drawing showing the appearance of a removable semi-conductor memory card (only henceforth a "memory card") in the PC.

[0009] PC102 is equipped with a display 103, a keyboard 104, and loudspeaker 106 grade, and is connected to the communication line 101 by the modem to build in. And the memory card writer 107 is inserted in card slots (memory card writer insertion opening 105), such as PCMCIA which this PC102 has. The memory card writer 107 is an adapter which connects PC102 and a memory card 109 electrically, and the memory card insertion opening 108 is equipped with the memory card 109.

[0010] By using such a system, a user can acquire the music data which the content provider on the Internet offers by passing through the following procedures. First, a user downloads a desired music content to the hard disk of the PC102 interior through a communication line 101. It is enciphered, and if music data remain as it is, they are unreproducible in PC102.

[0011] In order to reproduce, it is necessary to pay money using a credit card etc. to the content provider of a downloading agency. If payment is finished, a password and right information can come to hand from a content provider. A password is key data required to cancel the enciphered music data. Right information is information which shows the playback conditions permitted to users who show the count of refreshable in PC, the count to a memory card which can be written in, and a refreshable period, such

as a playback term.
[0012] The user who acquired a password and right information enters the password which came to hand from a keyboard 104 to the application program (this program is only hereafter called "application".) of dedication to which the copyright protection feature was attached, when carrying out the playback output of the music from the loudspeaker 106 of PC102. Then, the application carries out a playback output as voice through a loudspeaker 106, decoding the enciphered music data using a password, after checking right information.
[0013] Moreover, when the writing to a memory card is permitted as right information, the application can write the enciphered music data, a password, and right information in a memory card 109. Drawing 2 is drawing showing the appearance of the recorded message sender for telephone (henceforth a "player") 201 of the pocket mold which uses this memory card 109 as a record medium.
[0014] The liquid crystal display section 203 and a manual operation button 202 are formed in the top face of a player 201, the communication link ports 213, such as USB for connecting with the memory card insertion opening 206 for detaching and attaching a memory card 109 and PC102 grade, are established in a near-side side, and the analog output terminal 204, the digital output terminal 205, and the analog input terminal 223 grade are prepared in the right lateral.
[0015] If it is in the condition that playback is permitted, based on the music data stored in the memory card 109, a password, and right information, after a player 201 reads and decodes the music data, it is changed into an analog signal, and through the headphone 208 connected to the analog output terminal 204, it will output as voice or it will output the music data under playback to the digital output terminal 205 with digital data.
[0016] Moreover, this player 201 can record the music data, the password, and right information which were downloaded with that PC102 on a memory card 109 by changing into digital data the sound signal of an analog inputted from the analog input terminal 223 through a microphone etc., recording on a memory card 109 or communicating with PC102 connected through the communication link port 213. That is, this player 201 has the function to replace PC102 shown in drawing 1 , and the memory card writer 107, about playback of the music data recorded on record and the memory card 109 of the music data to a memory card 109.
[0017] Drawing 3 is the block diagram showing the hardware configuration of PC102. PC102 USB for connecting with the modem port for connecting with ROM111, RAM112, the display 103, and communication line 101 which have memorized beforehand CPU110, device key 111a, control program 111b, etc., or a player 201 etc. The memory card writer 107 which connects the communication link port 113 which it has, a keyboard 104, an internal bus 114, and a memory card 109 and an internal bus 214, the descrambler 1117 which decodes the encryption music data read from the memory card 109, and the decoded music data The AAC decoder 118 based on MPEG 2-AAC (ISO 13818-7) to elongate, D/A converter 119 which changes the elongated digital music data into an analog sound signal, a loudspeaker 106 and file management software, and application It consists of stored hard disk 120 grades.
[0018] This PC102 is performing file management software stored in the hard disk 120. It not only can use as an auxiliary storage unit which has the file system (ISO9293 grade) which became independent like a hard disk about the memory card 109, but By performing above-mentioned exclusive application stored in the hard disk 120 The modem of the communication link port 113 etc. is minded. Download a music content etc. from a communication line 101, or After performing mutual recognition with a memory card 109, a music content etc. is stored in a memory card 109, or the music content stored in the memory card 109 is read, and a playback output is carried out at a loudspeaker 106.
[0019] In addition, device key 111a stored in ROM111 is used for mutual recognition etc. so that it may be the private key of a proper and may mention later to this PC102. Drawing 4 is the block diagram showing the hardware configuration of a player 201. A player 201 The communication link ports 213, such as USB for connecting with ROM211, RAM212, the liquid crystal display section 203, and PC102 grade which have memorized beforehand CPU210, device key 211a, control program 211b, etc., a manual operation button 202, an internal bus 214, A memory card 109 and an internal bus 214 The card I/F section 215 to connect, the authentication circuit 216 which performs mutual recognition with a

memory card 109, the descrambler 217 which decodes the encryption music data read from the memory card 109, decoded MPEG 2-AAC which carries out music data elongation The analog music signal inputted from the AAC decoder 218 based on (ISO 13818-7), D/A converter 219 which changes the elongated digital music data into an analog sound signal, the loudspeaker 224, and the analog input terminal 223 A/D converter 221 which changes into digital music data, and its digital music data are based on MPEG 2-AAC (ISO 13818-7). It consists of the AAC encoder 220 which carries out compression coding, the scrambler 222 which enciphers the music data by which compression coding was carried out, an analog output terminal 204, a digital output terminal 205, and an analog input terminal 223.

[0020] It is loading control program 211b stored in ROM211 to RAM212, and performing CPU210, and this player 201 reads the music content stored in the memory card 109, and a playback output is carried out or it stores in a loudspeaker 224 the music content inputted through the analog input terminal 223 or the communication link port 213 at a memory card 109. That is, it can record music individually, or it can reproduce and it not only can enjoy itself, but it can perform record and playback of the music content concerning the electronic music distribution downloaded with PC102 (protection of copyrights is needed) like the usual player.

[0021] Drawing 5 is drawing showing the appearance and hardware configuration of a memory card 109. The memory card 109 is carrying out the internal organs of the rewritable nonvolatile memory which can write in repeatedly, and the storage capacity is 64MB and it operates in response to the power source of 3.3V, and supply of a clock signal from the exterior. Moreover, memory cards 109 are 2.1mm in thickness, 32mm long, and a 24mm wide rectangular parallelepiped configuration, they are written in the side face, have a prevention switch (write protect SW), and are electrically connected with an external instrument by the connection terminal of nine pins.

[0022] This memory card 109 builds in three IC chips (control IC 302, a flash memory 303, ROM304). It has the non-attesting field 331 grade which are the authentication field 332 which is a storage region which permits access only to the device which was able to be attested with a flash memory 303 being the nonvolatile memory which can rewrite a package elimination mold, and being a just device as a logical storage region, and the storage region which permits access, without needing such authentication. Here, since the authentication field 332 stores the important data in connection with protection of copyrights, it is used, and the non-attesting field 331 is used as an auxiliary storage unit in a general computer system. In addition, these two storage regions are classified bordering on the fixed address on a flash memory 303.

[0023] ROM304 has the read-only storage region called a special field, and has held beforehand the information on the manufacture manufacture name 342 grade of the media ID 341 which are the identification information of a proper, and this memory card 109 to this memory card 109. In addition, it is discernment data of the proper which can specify self in distinction from other semi-conductor memory cards, and media ID 341 are used for the mutual recognition between devices, and they are used here in order to prevent unjust access to the authentication field 332.

[0024] Control IC 302 is a control circuit which consists of active components (logic gate etc.), and has the authentication section 321, the command judging control section 322, the master key storage section 323, the special field access-control section 324, the authentication field access-control section 325, the non-attesting field access-control section 326, and a code and decryption circuit 327 grade. The authentication section 321 is a circuit which performs mutual recognition of the phase hand-loom machine which is going to access this memory card 109, and a challenge response mold, and attests the justification of a phase hand-loom machine by detecting whether it has a random number generator, a code machine, etc., and the phase hand-loom machine has the same code machine as that code machine. With in addition, the mutual recognition of a challenge response mold Challenge data in a phase hand-loom vessel in order to verify the justification of a phase hand-loom machine Delivery, The response data with which **** generation of the processing which proves self justification in a phase hand-loom machine to it was carried out in **** From a phase hand-loom machine to reception It is that both devices perform mutually the authentication step of judging whether a phase hand-loom machine being

attested by comparing these challenge data with response data.
[0025] The command judging control section 322 is a controller which consists of a decoding circuit which judges and performs the class of command (instruction to this memory card 109) inputted through the command pin, or a control circuit, and controls the various components 321-327 according to the class of inputted command. a command -- the data of a flash memory 303 -- reading - writing - not only the command to eliminate but the commands (an address space, command about non-eliminated data, etc.) for controlling a flash memory 303 are contained.
[0026] For example, about R/W of data, the command "SecureRead address count" for accessing the authentication field 332, "SecureWrite address count", the command "Read address count" for accessing the non-attesting field 331, "Write address count", etc. are defined. Here, "address" is the number of the sector of the beginning of a series of sector groups set as the object of R/W, and "count" shows the number of sum total sectors to write. Moreover, a sector is a unit at the time of writing data to a memory card 109, and is 512 bytes here.
[0027] The master key storage section 323 has memorized beforehand master key 323a used in order for a phase hand-loom machine to use in the case of mutual recognition or to protect the data in a flash memory 303. The special field access-control section 324 is a circuit which reads the media ID341 grade stored in the special field (ROM304).
[0028] The authentication field access-control section 325 and the non-attesting field access-control section 326 are circuits which perform data writing and read-out to the authentication field 332 and the non-attesting field 331 of a flash memory 303, and data are transmitted, respectively and received between external instruments (PC102 and player 201 grade) through four data pins. In addition, when rewriting the contents of the flash memory 303, a block (32 sectors, 16 K bytes) is outputted [these access-controls sections 325 and 326 / although it has the buffer memory for 1 block inside and a sector is logically outputted and inputted as a unit (access on a command with an external instrument)] and inputted as a unit. When rewriting one certain sector data, while reading the block which corresponds from a flash memory 303 to buffer memory and specifically carrying out package elimination of the block, after rewriting the applicable sector in buffer memory, the block is returned to a flash memory 303 from buffer memory.
[0029] It is the circuit which performs encryption and a decryption using master key 323a stored in the master key storage section 323 under control by the authentication field access-control section 325 and the non-attesting field access-control section 326, in case a code and the decryption circuit 327 write data in a flash memory 303, it enciphers and writes in the data, and when it reads data from a flash memory 303, it decrypts the data. This is for preventing a malfeasance, such as stealing the password which the inaccurate user decomposed this memory card 109, analyzed the contents of the flash memory 303 directly, and was stored in the authentication field 332.
[0030] In addition, control IC 302 has the synchronous circuit which generates the internal clock signal which synchronized with the clock signal supplied from a clock pin besides these main components 321-327, and is supplied to each component, an volatile storage region, the storage region of a non-volatile, etc. Moreover, in order to prevent the alteration of the information stored in the special field (ROM304), the ROM304 may be made to build in in control IC 302, or those information may be stored in a flash memory 303, and the special field access-control section 324 may apply a limit so that it cannot write in from the outside. It is good also as then storing the data enciphered in the code and the decryption circuit 327.
[0031] Drawing 6 is drawing showing the class of storage region of the memory card 109 seen from PC102 or the player 201. The storage region which a memory card 109 has is roughly divided, and are three fields, the special field 304, the authentication field 332, and the non-attesting field 331. The special field 304 is a read-only field, and reads to the data in this using a device dependent command. The authentication field 332 is a field whose R/W is possible, only when authentication is successful between PC102 or a player 201, and a memory card 109, and the enciphered command is used for it about access to this field. The non-attesting field 331 is a field which can be written without accessing namely, attesting by the command exhibited [SCSI / ATA,]. Therefore, to the non-attesting field 331,

R/W of data is possible by the file management software on PC102 like a flash plate ATA and CompactFlash (trademark).

[0032] It supposes that the following information is stored and three storage regions are provided with the function and the function of protection of copyrights to the music data concerning an electronic music distribution as an auxiliary storage unit of common PC by this. That is, the user data 427 grade which is common data with unrelated encryption contents 426 as which the music data set as the object of protection of copyrights were enciphered and protection of copyrights is stored in the non-attesting field 331. The cryptographic key 425 used as the private key for decoding the encryption contents 426 stored in the non-attesting field 331 is stored in the authentication field 332. And the media ID 341 which are the information needed in order to access the authentication field 332 are stored in the special field 304.

[0033] PC102 and a player 201 read the media ID 341 first stored in the special field 304 of the memory card 109 with which it was equipped, and take out the cryptographic key 425 and right information which were stored in the authentication field 332 using it. If playback is permitted using these cryptographic keys 425 or right information, it is reproducible, reading the encryption contents 426 in the non-attesting field 331, and decoding by the cryptographic key 425.

[0034] A certain user writes only the music data which came to hand unjustly in the non-attesting field 331 of a memory card 109 in PC102 grade, and presupposes that the player 201 tended to be equipped with such a memory card 109, and it was going to reproduce. However, although music data are stored in the non-attesting field 331 of the memory card 109, since the cryptographic key 425 or right information corresponding to the authentication field 332 do not exist, the player 201 cannot reproduce the music data. Since the music content is not reproduced even if it reproduces only a music content to a memory card 109 by this without being accompanied by the cryptographic key and right information on normal, the unjust duplicate of a digital work is prevented.

[0035] (a) shows the Ruhr in access to each field, drawing 7 is drawing showing the limit at the time of PC102 and a player 201 accessing each field of a memory card 109, and the gestalt of a command, and (c) is [(b) shows the Ruhr in modification of the size of each field, and] the conceptual diagram showing the field of a memory card 109. The special field 304 is a read-only field, and can be accessed by the device dependent command, without attesting. The media ID 341 stored in this special field 304 are used for the generation and the decode of an encryption command for accessing the authentication field 332. That is, PC102 and a player 201 read these media ID 341, encipher the command which accesses the authentication field 332 using this, and send it to a memory card 109. On the other hand, the memory card 109 which received the encryption command decodes, interprets and executes the encryption command using media ID 341.

[0036] The authentication field 332 is a field whose access is attained, only when authentication is successful between the equipment and the memory cards 109 which access the memory card 109 of PC102 or player 201 grade, and the magnitude is equivalent to the sector of an individual (YYYY+1). that is, logically, this authentication field 332 consists of sectors of the 0th - YYYY -- having -- physical -- the [of a flash memory 303] -- it consists of sectors which have the sector address of XXXX - ** (XXXX+YYYY). In addition, sector addresses are a series of numbers uniquely attached to each of all sectors that constitute a flash memory 303.

[0037] The non-attesting field 331 can be accessed by standard commands, such as ATA and SCSI, without attesting, and the magnitude is equivalent to the sector of XXXX individual. That is, also logically and physically, this non-attesting field 331 consists of the 0th - (XXXX-1) a sector. In addition, the alternative block field 501 which consists of an assembly of the shift block for substituting for the defective block (block which has the storage region of the defect who cannot write normally) produced to the authentication field 332 or the non-attesting field 331 may be beforehand assigned to a flash memory 303.

[0038] Moreover, although the special field 304 can be accessed without authentication, in order to prevent the analysis from an inaccurate user, though it cannot access unless it comes out, after attesting, it is good, and the command which accesses the special field 304 may be enciphered. next, drawing 7 (b)

and (c) -- using -- the authentication field 332 and the non-attesting field 331 -- how to change each area size is explained.

[0039] Although the memory capacity of the sum total of the authentication field 332 and the non-attesting field 331 which are established in a flash memory 303 is the fixed value except all the storage regions of a flash memory 303 to alternative block field 501 grade, a part for i.e., the sector of an individual (XXXX+YYYY +1), each magnitude is changing the value of the boundary address XXXX, and serves as adjustable.

[0040] In order to change area size, it attests first. This is because magnitude cannot be easily changed using the software which performs standard program wide opened widely by the user of PC, and unjust access. After attesting, it is the device dependent command of field modification, and the magnitude (the new number XXXX of sectors) of the non-attesting field 331 is sent to a memory card 109.

[0041] If the field change command is received, a memory card 109 will save the value XXXX in a working area [**** / in a memory card 109 / un-] etc., and will perform the access control to the authentication field 332 and the non-attesting field 331 by making the value into the new boundary address in subsequent accesses. that is, -- while assigning the physical sector of the 0th - XXXX on a flash memory 303 to the non-attesting field 331 -- the -- the sector of eye watch [XXXX - (XXXX+YYYY)] is assigned to the authentication field 332. And based on such new memory mapping, the access-control sections 325 and 326 change the logical address and a physical address, or supervise generating of violation of access exceeding a field. In addition, the logical address is the address in the data space (on a command) at the time of seeing a memory card 109 from an external instrument, and a physical address is the address in the data space which has the flash memory 303 of a memory card 109.

[0042] Here, when size of the authentication field 332 is enlarged by making the boundary address small, in order to maintain logical compatibility with modification before, the allowance of moving all the data stored in the authentication field 332 is needed. For that purpose, what is necessary is only for the movement magnitude of the boundary address to move all data in the direction of low order of the address (copy), and just to change correspondence relation, for example so that a new physical address may be equivalent to the logical address which begins from the new boundary address. The data space is expanded maintaining the logical address of the data stored in the authentication field 332 by this.

[0043] In addition, it is good also as enciphering and using a command also about the device dependent command for field modification from a viewpoint which prevents unjust access. Drawing 8 is the flow Fig. showing the actuation in which PC102 (and player 201) writes contents, such as music data, in a memory card 109. Here, the case (S601) where PC102 writes in a memory card 109 is explained.

[0044] (1) If PC102 performs authentication of the authentication section 321 of a memory card 109, and a challenge response mold and succeeds in the authentication using device key 111a etc., it will take out master key 323a from a memory card 109 first (S602).

(2) Next, take out the media ID 341 stored in the special field 304 of a memory card 109 using a device dependent command (S603).

[0045] (3) Then, generate a random number and generate the password for enciphering music data from the random number, and master key 323a and Media ID 341 which were taken out now (S604). For example, in the above-mentioned authentication, what enciphered the challenge data (random number) transmitted to the memory card 109 is used for the random number at this time.

(4) Encipher the obtained password by master key 323a and media ID 341, and write in the authentication field 332 as a cryptographic key 425 (S605). At this time, before transmitting data (cryptographic key 425), the command for writing in the authentication field 332 is enciphered, and it transmits to the memory card 109.

[0046] (5) Finally store in the non-attesting field 331 as encryption contents 426, enciphering music data with a password (S606). Drawing 9 is the flow Fig. showing the actuation which reads contents, such as music data, from a memory card 109, and is reproduced by the player 201 (and PC102). Here, the case (S701) where a player 201 reproduces the music data in a memory card 109 is explained.

[0047] (1) If a player 201 performs authentication of the authentication section 321 of a memory card

109, and a challenge response mold and succeeds in the authentication using device key 211a etc., it will take out master key 323a from a memory card 109 first (S702).
(2) Next, take out the media ID 341 stored in the special field 304 of a memory card 109 using a device dependent command (S703).
[0048] (3) Then, take out the music data encryption key 425 from the authentication field 332 of a memory card 109 (S704). At this time, the command for reading from the authentication field 332 is enciphered in advance of read-out of data (cryptographic key 425), and it transmits to the memory card 109.
(4) Decrypt the obtained cryptographic key 425 by master key 323a and media ID 341, and extract a password (S705). The decryption at this time is the inverse transformation of encryption at step S605 shown in drawing 8 .
[0049] (5) Finally, read the encryption contents 426 from the non-attesting field 331, and play music, decoding with the password extracted at the above-mentioned step S705 (S706). Thus, the music data stored in the non-attesting field 331 of a memory card 109 cannot be decoded if there is no cryptographic key 425 of the authentication field 332. Therefore, since the music data is normally unreproducible even if it copies only music data to injustice at another memory card, the copyright of the music data is protected by insurance.
[0050] Moreover, since access to the authentication field of a memory card is permitted, the protection of copyrights of permitting access to the authentication field of a memory card only to the device which filled certain conditions with choosing appropriately a device key, encryption algorithm, etc. which are used for authentication, and using them only of the device which succeeded in authentication becomes possible. In addition, although the password used for that encryption was enciphered by the master key and Media ID and it was stored in the authentication field 332 as a cryptographic key in this example when recording encryption contents on a memory card 109 (S605), it is good also as enciphering using either a master key and the media ID. The advantage that the circuit scale of a memory card 109 or player 201 grade becomes small with simplification of encryption by this although there is a possibility that the reinforcement of a code may fall is acquired.
[0051] Moreover, according to authentication, although the player 201 and PC102 took out master key 323a from the memory card 109, they may embed the master key 323a beforehand at a player 201 or PC102, may encipher master key 323a, and may store it in the special field 304 as an encryption master key. Next, the example which stored "the count of read-out", and the example which stored "the count of digital output authorization" are shown as an example of an activity of the authentication field of such a memory card.
[0052] Drawing 10 is the flow Fig. showing the actuation in which the player 201 (and PC102) was stored in the authentication field of a memory card 109, and which reads and operates a count 812. Here, the case (S801) where reproducing the music data which were stored in the memory card 109 and with which the player 201 was stored in the non-attesting field 331 of a memory card 109 to a sound signal is permitted is explained only within the limits of a count 812 by reading.
[0053] (1) If a player 201 performs authentication of the authentication section 321 of a memory card 109, and a challenge response mold and succeeds in the authentication using device key 211a etc., it will take out master key 323a from a memory card 109 first (S802).
(2) Next, take out the media ID 341 stored in the special field 304 of a memory card 109 using a device dependent command (S803).
[0054] (3) Then, take out the music data encryption key 425 from the authentication field 332 of a memory card 109 (S704). At this time, the command for reading from the authentication field 332 is enciphered in advance of read-out of data (cryptographic key 425), and it transmits to the memory card 109.
(4) Next, read from the authentication field 332 of a memory card 109, take out a count 812, and inspect the value (S804). Consequently, when it is the value of the purport to which read-out with the unrestricted value is permitted, music is played according to the procedure (S704-S706) shown in drawing 9 , and the same procedure (S806-S808).

[0055] (5) On the other hand, when the count 812 of read-out shows 0, judge with playback not being permitted any longer (S805), and end regeneration (S809). When that is not right, the one count 812 of read-out is subtracted, and after returning the result to the authentication field 332, music is played according to (S805) and the above-mentioned procedure (S806-S808).
[0056] Thus, it becomes possible to control the count of the music playback by the player 201 by [which specified the count of playback permitted beforehand as the authentication field 332 of a memory card 109] reading and storing the count 812. It becomes possible to apply to the analog playback by for example, the rental CD, a KIOSK terminal, etc. by this.
[0057] In addition, it can replace with the count 812 of read-out, and the total time amount which can reproduce a music content can also be restricted by considering as "read-out time amount." Moreover, a count and time amount may be combined. Furthermore, the count 812 of read-out may subtract the count, only when continuing being reproduced exceeding fixed time amount, such as 10 etc. seconds, after starting playback. Moreover, the count 812 of read-out is good also as enciphering and storing, in order to prevent an unjust alteration.
[0058] Drawing 11 is the flow Fig. showing the actuation which operates the count 913 of digital output authorization by which the player 201 (and PC102) was stored in the authentication field of a memory card 109. Here, the case (S901) where it is permitted that a player 201 reads and carries out the digital output of the music data stored in the non-attesting field 331 of a memory card 109 only within the limits of the count 913 of digital output authorization stored in the memory card 109 is explained.
[0059] (1) A player 201 extracts the password which takes out master key 323a like the case (S701-S705) of the playback shown in drawing 9 after attesting with a memory card 109 (S902), takes out media ID 341 (S903), and takes out a cryptographic key 425 (S904) (S905).
(2) Next, take out the count 913 of digital output authorization from the authentication field 332 of a memory card 109, and inspect the value (S906). Consequently, when it is the value of the purport to which a digital output with the unrestricted value is permitted, the encryption contents 426 are read from the non-attesting field 331, and it outputs from the digital output terminal 205 as digital music data, decoding with the password extracted at the above-mentioned step S905 (S909).
[0060] (3) On the other hand, when the count 913 of digital output authorization shows 0, judge with the digital output not being permitted any longer (S908), and perform only playback by analog output (S908). That is, the encryption contents 426 are read from the non-attesting field 331, and music is played, decoding with a password (S908).
(4) When the fixed count of a limit whose count 913 of digital output authorization which it began to read is not 0 is shown, read the encryption contents 426 from (S907) and the non-attesting field 331 after subtracting the one count and returning the result to the authentication field 332, and output from the digital output terminal 205 as digital music data, decoding with the password extracted at the above-mentioned step S905 (S909).
[0061] Thus, it becomes possible to control the count of the digital output of the music data based on a player 201 by storing the count 913 of digital output authorization which specified the count of the digital output permitted beforehand as the authentication field 332 of a memory card 109. By this, the application to the digital playback by for example, the rental CD, a KIOSK terminal, etc., i.e., employment which permits a copy by the count which specified digital dubbing of the music data memorized to the memory card as the origin of comprehension of a copyright person, is realized.
[0062] In addition, like the case of "the count of read-out", it can replace with the count 913 of digital output authorization, and the total time amount which can output a music content with digital data can also be restricted by considering as "digital output authorization time amount." Moreover, a count and time amount may be combined. Furthermore, after the count 913 of digital output authorization starts the output, only when continuing being outputted exceeding fixed time amount, such as 10 etc. seconds, it may subtract the count. Moreover, the count 913 of digital output authorization is good also as enciphering and storing, in order to prevent an unjust alteration.
[0063] Furthermore, the function in which only the count specified by a copyright person increases the count of digital output authorization by paying price into a copyright person may be added. Next, the

physical DS (a sector and structure of an ECC block) of this memory card 109 is explained. In this memory card 109, suitable DS to prevent the malfeasance accompanying backup and restoration of the data stored in the flash memory 303, the malfeasance accompanying the alteration of data, etc. is adopted. That is, above "counts of read-out" and "the counts of digital output authorization" may be stored in the authentication field 332, and the following attacks may be received by the method counted down whenever it performs these actions.

[0064] That is, when music playback is repeated and these counts are set to 0 after backing up the stored data of the flash memory 303 whole to an external auxiliary storage unit etc., by restoring backup data, music playback can be repeated again or it is possible [it] to repeat music playback unjustly altering the "count of read-out" itself. Therefore, the allowance which prevents such an action is needed.

[0065] Drawing 12 is drawing showing DS common to the authentication field 332 and the non-attesting field 331 of a memory card 109, and the flow of the R/W processing corresponding to the DS. the counter value which the random number generator 1003 which the authentication section 321 grade of control IC 302 has generates here -- the time -- as a strange key -- using -- having .

[0066] 16 bytes of extended partition 1005 is assigned to a flash memory 303 512 bytes of every sector 1004. The data with which each sector was enciphered with the counter value are stored. An extended partition 1005 consists of a strange field 1007 at the time of 8 bytes for storing the counter value used for generation of the 8 bytes of ECC data 1006 and encryption data for storing the error correcting code of the encryption data stored in the corresponding sector.

[0067] In addition, logically (using the command wide opened by the user), an accessible field is only a sector 1004 and an extended partition 1005 is a field where it is accessible that it is only physical (as control by the equipment which write a memory card). even if only sector data are altered by considering as such DS using a command etc. -- the time -- strange -- since the contents of field 1007 are not changed, an unjust alteration can be prevented by using those adjustments.

[0068] Specifically, PC102 and a player 201 store or read data to the authentication field 332 and the non-attesting field 331 of a flash memory 303 according to the following procedures every sector 1004. Here, a procedure in case PC102 writes data in a memory card 109 (S1001) is explained first.

(1) PC102 requires issue of a counter value from a memory card 109. Then, the control IC 302 in a memory card 109 generates a random number with the internal random number generator 1003 (S1005), and sends it to PC102 grade by making the random number into a counter value (S1002).

[0069] (2) Generate a password from the acquired counter value, and master key 323a and Media ID 341 which are already acquired (S1003).

(3) Send to a memory card 109, enciphering with a password the data for 1 sector which should be written in (S1004). At this time, the (4) memory card 109 which also sends the information which specifies the sector which should be written in, and the counter value used for encryption together writes the received encryption data in the specified sector 1004 (S1006).

[0070] (5) Calculate ECC from the encryption data and write in the extended partition 1005 corresponding to the above-mentioned sector as ECC data 1006 (S1007).

(6) then, the counter value received with the above-mentioned encryption data -- the time -- strange -- write in field 1007 (S1008).

Next, a procedure in case PC102 reads data from a memory card 109 (S1011) is explained.

[0071] (1) PC102 specifies a sector to a memory card 109 -- require both read-out of data. Then, a memory card 109 reads only the encryption data of the specified sector 1004 first, and outputs them to PC102 (S1016), and PC102 receives the encryption data (S1012).

(2) Next, a memory card 109 reads the counter value stored in the strange field 1007 at the time of the extended partition 1005 corresponding to the specified sector 1004, and outputs it to PC102 (S1017), and PC102 receives the counter value (S1013).

[0072] (3) Generate a password from the counter value which it began to read, and master key 323a and Media ID 341 which are already acquired (S1014).

(4) Decode encryption data using the password (S1015).

the case where the data of a sector 1004 are changed by the unjust alteration etc. here -- the time --

strange -- mismatching with the counter value read from field 1007 arises, and it is not restored to the original data.

[0073] Thus, from a user, the strange field 1007 can be formed in a flash memory 303 at the time as a hiding (it cannot access) field which is not visible, and the alteration of the data by the inaccurate user can be prevented by enciphering and storing data with the password depending on the counter value stored there. in addition -- here -- the time -- strange -- although field 1007 considered as the extended partition 1005 for storing ECC, as long as it is a field whose rewriting is impossible from the exterior of a memory card, it may be prepared in other fields in a flash memory 303.

[0074] Moreover, although the counter value was a random number, it is good also as a value which considers as timer values, such as time of day which changes every moment, or shows the count of writing to a flash memory 303. Next, a desirable example is explained about matching with the logical address of a flash memory 303, and a physical address. Drawing 13 is drawing showing signs that correspondence with the logical address and a physical address is changed, and the translation table 1101 corresponding to [(a)] (a) in (c) and (d) show the translation table 1101 corresponding to (b) corresponding to the correspondence relation after modification in the correspondence relation before modification, and (b).

[0075] Here, it is the table which makes a group all the logical addresses (here number of a logical block), and the physical address (number of the physical block which constitutes a flash memory 303 here) corresponding to each logical address, and memorizes them, a translation table 1101 is saved in a storage region [**** / in control IC 302 / un-] etc., and in case the logical address is changed into a physical address by the authentication field access-control section 325 or the non-attesting field access-control section 326, it is referred to.

[0076] The device which accesses a memory card 109 can write data in not all the data space (all physical blocks that constitute a flash memory 303) that exists physically in a memory card 109, but can write data only in the logical data space (logical block) which can be pinpointed with the logical address. One of the reason of this is because the alternative field for replacing that field must be secured when it becomes impossible to write by damaging a part of flash memory 303. And since the logical continuity of a file it is discontinuous by reflecting modification of the matching in a translation table from the physical block which plurality follows is maintained even if it is the case where such a defective block is replaced with the block in an alternative field, it can be pretended that breakage did not arise to the external instrument.

[0077] However, if it has repeated storing in a memory card 109 the file which consists of two or more blocks, or deleting it, the fragmentation of a logical block will increase. That is, as shown in drawing 13 (a), in spite of being the logical block which constitutes the same file file1, those logical addresses will become discontinuity.

[0078] Now, since it cannot write to the logical continuation field of a memory card 109 for example, when it is going to store music data in a memory card 109, it will be necessary to publish a write command "Write address count" for every block, and drawing speed will fall. Similarly, in spite of being music data which constitute one music also in read-out actuation, it will be necessary to read for every block and to publish a command "Read address count", and real-time playback of music data will be difficult.

[0079] As an approach of solving this problem, the control IC 302 of this memory card 109 has the function which rewrites a translation table 1101 based on the command from an external instrument. Specifically, the command judging control section 322 of control IC 302 will rewrite a translation table 1101 using the parameter which interprets the command and is sent continuously, if the device dependent command for rewriting a translation table 1101 is inputted from a command pin.

[0080] The concrete actuation is as being shown in drawing 13 . Before the above-mentioned device dependent command is sent now, as a flash memory 303 is shown in drawing 13 (a), the data which constitute a file file1 exist in physical addresses 0 and 2, and suppose that the data which constitute a file file2 in a physical address 1 exist. And as shown in a translation table 1101 at drawing 13 (c), suppose that the contents a physical address and whose logical address correspond are held. That is, suppose that

the data of a file file2 are inserted into the data of another file file1, and are stored on the logical address like a physical address top.
[0081] the external instrument which will be obtained and carried out if I will cancel such a condition sends the above-mentioned device dependent command and parameter which show the purport which secures the continuity of the specific file file1 to a flash memory 303. Then, the command judging control section 322 of a memory card 109 rewrites a translation table 1101 by the contents shown in drawing 13 (d) according to the device dependent command and parameter. That is, the logic of a flash memory 303 and the correspondence relation of a physical address are changed as shown in drawing 13 (b).
[0082] As shown in the related Fig. shown in drawing 13 (b), although arrangement of a physical block is not changing, it is rearranged so that two logical blocks which constitute a file file1 may continue. By this, the external instrument is that a twist can also access a file file1 at a high speed till then after next access.
[0083] the authentication field 332 of not only in order that modification of the above translation tables 1101 may fix the fragmentation of a logical block, but the flash memory 303, and the non-attesting field 331 -- it is used also when changing each size. Since what is necessary is just to rewrite a translation table 1101 so that it may be assigned as a physical block of the field where the physical block of the field which makes size small enlarges size at this time, high-speed field modification is attained.
[0084] Next, the function about the non-eliminated block which this memory card 109 has, and the actuation at the time of specifically receiving a non-eliminated list command and an elimination command are explained. Here, a non-eliminated block is a physical block in a flash memory 303, writing was performed in the past and the block which is in the condition of not eliminating, physically is said. That is, a non-eliminated block is a physical block for which package elimination is needed, before being used for a degree (written in).
[0085] Moreover, the command judging control section 322 is one of the commands in which an interpretation and activation are possible, and a non-eliminated list command is a command for acquiring the list of the numbers of all non-eliminated blocks that exist in the flash memory 303 at the time. Before the flash memory 303 currently used for the memory card 109 writes in, package elimination in a block unit is needed, but since the elimination processing occupies about the one half of write-in time amount, the direction eliminated beforehand can write it in a high speed more. Then, this memory card 109 provides the external instrument with the non-eliminated list command and the elimination command, in order to give those facilities.
[0086] Now, let a flash memory 303 be the busy condition of a logical block as shown in drawing 14 (a), and a physical block. Here, logical blocks 0-2 are using it, and physical blocks 0-2, and 4 and 5 have become a non-eliminated block. In this condition, the non-eliminated list 1203 currently held in the command judging control section 322 serves as contents shown in drawing 14 (b). Here, the non-eliminated list 1203 is a storage table which consists of an entry corresponding to all the physical blocks that constitute a flash memory 303, and the value (in "0" and not eliminating, it is "1" when finishing [elimination]) according to the elimination condition of a corresponding physical block is held under control by the command judging control section 322.
[0087] Drawing 14 (c) is the flow Fig. showing actuation in case PC102 and a player 201 eliminate a block in advance using a non-eliminated list command and an elimination command in such a condition. In addition, as shown in drawing 14 (d), tables, such as FAT (File Allocation Table) which shows the busy condition of a logical block, shall be stored in a flash memory 303.
[0088] PC102 and the external instrument of player 201 grade publish a non-eliminated list command to this memory card 109 in the idle time which access to a memory card 109 has not generated (S1201). The command judging control section 322 of the memory card 109 which received the command is referring to the non-eliminated list 1203 which it has inside, specifies the numbers 0-2 of the physical block into which status value 1 is registered, and 4 and 5, and returns it to the external instrument.
[0089] Then, an external instrument is referring to the table showing the busy condition of the logical block shown in drawing 14 (d) stored in the flash memory 303, and the block which is not used logically

is specified (step S1202). And based on the information acquired at the two above-mentioned steps S1201 and S1202, an eliminable block, i.e., the elimination command which specified the number of these blocks 4 and 5 to (step S1203) and a memory card 109 after specifying a block [**** / un-] (here, they are physical blocks 4 and 5) physically [did not use it logically and], is published (step S1204). The command judging control section 322 of the memory card 109 which received the command carries out package elimination of the physical blocks 4 and 5 specified by taking out directions to the access-control sections 325 and 326 etc.

[0090] Since the elimination processing to the physical block becomes unnecessary by this when the writing to the physical blocks 4 and 5 occurs, high-speed writing is attained. Next, the function about protection of the personal data which this memory card 109 has, and in case a memory card 109 specifically attests an external instrument, the protection feature of the personal data in the case of needing the personal data of the user who uses that external instrument is explained. Here, personal data are data for identifying the user uniquely, and are data for making a memory card 109 identify as a user of normal to whom access to the authentication field 332 of a memory card 109 was permitted.

[0091] In such a case, it sets and there is un-arranging [which requires the thing to the authentication field 332 for which personal data are repeatedly inputted at every access to a user, is intercepted by the inaccurate person in our having decided to store the personal data in the authentication field 332, or is looked at by other users who have the authority to access the authentication field 332].

[0092] In order to prevent this, how to store after enciphering about personal data as well as music data with the password which the individual set up can be considered. However, when a password is set up, whenever it sees the personal data, a password must be entered, a procedure is troublesome and the management is also needed. Then, this memory card 109 has the function to avoid repeating and inputting personal data superfluously.

[0093] Drawing 15 is drawing showing the communication link sequence and the main components between the player 201 for authentication, and a memory card 109. In addition, processing shown in this Fig. is mainly realized by the authentication circuit 216 of a player 201, and the authentication section 321 of a memory card 109. As shown in this Fig., the authentication circuit 216 of a player 201 has remembered beforehand device-dependent [which is ID of a proper / ID / 1302] to be the master key 1301 which is the same private key as master key 323a held at the memory card 109 other than functions, such as encryption and a decryption, to the players 201, such as a serial number (second/n).

[0094] Moreover, otherwise, the authentication section 321 of a memory card 109 has the device-dependent ID group storage region 1310 and the user key storage region 1311 which are two storage regions [**** / un-] in functions, such as encryption, a decryption, and a comparison. The device-dependent ID group storage region 1310 is a storage region for memorizing device-dependent [of all the devices by which access to the authentication field 332 of this memory card 109 was permitted / ID], and the user key storage region 1311 is a storage region for memorizing the user key sent from the device as personal data.

[0095] The concrete authentication procedure is as follows. In addition, in transmission and reception, it is enciphered and transmitted and all data are decoded by the receiving side. And the key used for encryption and a decryption with the following procedure whenever a procedure progresses is generated.

(1) If a memory card 109 and a player 201 are connected, first, a player 201 will encipher device-dependent [ID / 1302] using the master key 1301, and will send it to a memory card 109.

[0096] (2) A memory card 109 inspects whether device-dependent [which was received / which was enciphered / ID / 1302] is decoded by master key 323a, and device-dependent [which was obtained / ID / 1302] is already stored in the device-dependent ID group storage region 1310.

(3) Consequently, notify the purport that authentication was successful when device-dependent [ID / 1302] was already stored to a player 201, and on the other hand, when device-dependent [ID / 1302] is not stored, require a user key from a player 201.

[0097] (4) After a player 201 demands the input of a user key from a user, it acquires the user key as personal data from a user, and sends the user key to a memory card 109.

(5) It stores in the device-dependent ID group storage region 1310 device-dependent [which was gained at the above-mentioned step (3) / ID / 1302] while a memory card 109 compares the sent user key with the thing beforehand stored in the user key storage region 1311, and it notifies the purport that authentication was successful to a player 201, when in agreement, or when the user key storage region 1311 is empty.

[0098] When the device and memory card 109 which a user owns are connected for the first time by this, the input of personal data (user key) is needed, but since device-dependent [of the device / ID] is used for 2nd henceforth and authentication is automatically successful, the input of personal data is not required again. Next, the modification of the Challenge Handshake Authentication Protocol of this memory card 109, and a PC102 and the external instrument of player 201 grade is explained using drawing 16 and drawing 17 .

[0099] Drawing 16 is the communication link sequence diagram showing the authentication procedure of the memory card 109 and external instrument (here player 201) concerning a modification. Processing here is mainly realized by the authentication section 321 of the control program 111b and the memory card 109 of the authentication circuit 216 of the player 201 concerning a modification, and PC102. moreover, the enciphered master key (encryption master key 323b) stores in the master key storage section 323 of a memory card 109 -- having -- **** -- the special field 304 -- media ID 341 -- in addition, the secure media ID 343 which encipher the media ID 341 and are obtained shall be stored

[0100] First, a player 201 is emitting a command to a memory card 109, takes out master key 323b of a memory card 109, and decodes it by device key 211a. A decode algorithm here corresponds to the cryptographic algorithm used when encryption master key 323b stored in the memory card 109 was generated. Therefore, if device key 211a which this player 201 has was planned (thing of normal), this decode will revert to the original master key.

[0101] Then, a player 201 is emitting a command to a memory card 109, takes out the media ID 341 of a memory card 109, and enciphers them with the restored above-mentioned master key. Cryptographic algorithm here is the same as that of the cryptographic algorithm used when the secure media ID 343 stored in the memory card 109 were generated. Therefore, the same secure media ID as the secure media ID 343 which a memory card 109 has are obtained by encryption here.

[0102] Then, a player 201 and a memory card 109 perform mutual recognition using each of these secure media ID. Consequently, also in which device, the information which shows whether it succeeded in authentication of a phase hand-loom machine (OK/NG), and the secure key which is a strange key when becoming settled depending on the authentication result are generated. This secure key has the property changed whenever it repeats mutual recognition only in accordance with the case where both devices 201 and 109 succeed in authentication.

[0103] Then, if it succeeds in mutual recognition, a player 201 will generate the command for accessing the authentication field 332 of a memory card 109. If it is the case where data are read from the authentication field 332, the parameter (the address "address" of 24 bit length and count of 8 bit length "count") of the command "SecureReadaddress count" will be enciphered with a secure key, and, specifically, the encryption command which connects the obtained encryption parameter and the tag (code of 6 bit length which shows the class "SecureRead" of command) of the command, and is obtained will be sent to a memory card 109.

[0104] The memory card 109 which received the encryption command judges the class of command from the tag. Here, it judges with it being a read-out command "SecureRead" from the authentication field 332. Consequently, when it judges with it being an access command to the authentication field 332, the parameter contained in the command is decoded with the secure key obtained by mutual recognition. Since a decode algorithm here corresponds to the cryptographic algorithm used when generating an encryption command in a player 201, if mutual recognition was successful (i.e., if the secure key used by both devices is in agreement), the parameter obtained by this decode will become equal to the original parameter used by the player 201.

[0105] And a memory card 109 reads the cryptographic key 425 stored in the sector specified with the decoded parameter from the authentication field 332, enciphers it with a secure key, and transmits to a

player 201. A player 201 decodes the sent data using the secure key obtained by mutual recognition. Since a decode algorithm here is equivalent to the algorithm used for encryption of a cryptographic key 425 in the memory card 109, if mutual recognition was successful (i.e., if the secure key used by both devices is in agreement), the data obtained by this decode are in agreement with the original cryptographic key 425.

[0106] In addition, a memory card 109 cancels the secure key used for it whenever it finished activation of the access command to the authentication field 332 (elimination). By this, whenever the external instrument which accesses the authentication field 332 of a memory card 109 sent out one command, it needed to perform mutual recognition in advance, and it needs to pass it to it. Drawing 17 is the communication link sequence diagram showing the detailed procedure in the mutual recognition shown in drawing 16 . Here, a memory card 109 and a player 201 perform mutual recognition of a challenge response mold.

[0107] In order to verify the justification of a player 201, a memory card 109 generates a random number and sends it to a player 201 by making it into challenge data. In order to prove self justification, a player 201 enciphers the challenge data and returns it to a memory card 109 as response data. A memory card 109 compares the response data with the encryption challenge data which encipher the random number sent as challenge data, and are obtained, when in agreement, recognizes it as (O.K.) which succeeded in authentication of a player 201, and receives the access command to the authentication field 332 sent from the player 201. On the other hand, the activation is refused, even if it has recognized it as having carried out (NG) which did not succeed in authentication and the access command from the player 201 to the authentication field 332 has been sent after that, when not in agreement as a result of a comparison.

[0108] Similarly, a player 201 performs the same exchange as the above-mentioned authentication, in order to verify the justification of a memory card 109. That is, a random number is generated and it sends to a memory card 109 by making it into challenge data. In order to prove self justification, a memory card 109 enciphers the challenge data, and returns it to a player 201 as response data. A player 201 compares the response data with the encryption challenge data which encipher the random number sent as challenge data, and are obtained, when in agreement, recognizes it as (O.K.) which succeeded in authentication of a memory card 109, and performs AKUSESUKO to the authentication field 332 of the memory card 109. On the other hand, when not in agreement as a result of a comparison, it is recognized as having carried out (NG) which did not succeed in authentication, and access to the authentication field 332 of the memory card 109 is given up.

[0109] In addition, the encryption algorithm in these mutual recognition is altogether the same as long as a memory card 109 and a player 201 are just devices. Moreover, a memory card 109 and a player 201 carry out EXCLUSIVE OR operation of the encryption challenge data and response data which were generated in each authentication and certification, and they are used for them by using the obtained result as a secure key for access to the authentication field 332 of a memory card 109. doing so -- things -- both sides -- a device -- 109 -- and -- 201 -- mutual recognition -- having succeeded -- a case -- being common -- ** -- becoming -- and -- the time -- being strange -- secure ones -- a key -- sharing -- suiting -- things -- being possible -- ** -- becoming -- this -- authentication -- a field -- 332 -- accessing -- conditions -- ****** -- mutual recognition -- succeeding -- **** -- things -- conditions -- ** -- carrying out -- having -- ******** .

[0110] In addition, it is good as a generation method of a secure key also as taking the exclusive OR of encryption challenge data, response data, and the secure media ID. Next, the modification about the modification function of the boundary line of the authentication field 332 of this memory card 109 and the non-attesting field 331 is explained using drawing 18 and drawing 19 . Drawing 18 is drawing showing the busy condition of the flash memory 303 before changing a boundary line. Drawing 18 (a) is a memory map in which the configuration of the physical block of a flash memory 303 is shown.

[0111] Drawing 18 (b) is the translation table 1103 of non-attesting field 331 dedication put on a storage region [**** / in the non-attesting field access-control section 326 / un-] etc., and the correspondence relation between the logical block of the non-attesting field 331 and a physical block is stored. By

referring to this translation table 1103, the non-attesting field access-control section 326 can change the logical address into a physical address, or can detect violation of access exceeding a quota field.
[0112] Drawing 18 (c) is the translation table 1102 of authentication field 332 dedication put on a storage region [**** / in the authentication field access-control section 325 / un-] etc., and the correspondence relation between the logical block of the authentication field 332 and a physical block is stored. By referring to this translation table 1102, the authentication field access-control section 325 can change the logical address into a physical address, or can detect violation of access exceeding a quota field.
[0113] As shown in drawing 18 (a) before modification of a boundary line, the physical block 0000 located in a lower address rather than a boundary line among the storage regions (a physical block 0000 - EFFF) except the alternative field of a flash memory 303 - DFFF are assigned to the non-attesting field 331, and the physical block E000 located in an upper address - EFFF are assigned to the authentication field 332.
[0114] And in the non-attesting field 331, as shown in the translation table 1102 shown in drawing 18 (b), it is matched so that the number of a physical block and a logical block may be in agreement. As shown on the other hand in the translation table 1103 shown in drawing 18 (c), in the authentication field 332, as for the physical block and the logical block, the list of the number is a reverse order. That is, a logical block 0000 - each 0FFF support physical block EFFF-E000. This is because the logical block took into consideration the time and effort of being used for ascending order, data evacuation of the physical block which field modification produced when a boundary line was moved, or migration processing.
[0115] Drawing 19 (a) - (c) is drawing showing the busy condition of the flash memory 303 after changing a boundary line, and corresponds to drawing 18 [before modification] (a) - (c), respectively. In addition, modification of a boundary line is realized when the command of the dedication which specifies the address is inputted into the command judging control section 322 from a command pin, and the translation table 1102 in the authentication field access-control section 325 and the translation table 1103 in the non-attesting field 331 are rewritten by the command judging control section 322.
[0116] Drawing 19 (a) As shown in - (c), the boundary line placed between a physical block E000 and DFFF is moved between a physical block D000 and CFFF here. That is, only 1000 (hex) individual decreases the size of the non-attesting field 331, and only 1000 (hex) is making the size of the authentication field 332 increase. In connection with it, as shown in drawing 19 (b), the size of the translation table 1103 of the non-attesting field 331 decreases an entered part of 1000 (hex) individuals, consequently the physical block 0000 corresponding to a logical block 0000 - CFFF - CFFF are shown. On the other hand, as shown in drawing 19 (c), it is increased by the size of the translation table 1102 of the authentication field 332 an entered part of 1000 (hex) individuals, consequently physical block EFFF-D000 corresponding to logical-block 0000-1FFF is shown.
[0117] Thus, it becomes possible by changing a non-attesting field and an authentication field according to a boundary line, and changing the size of each field by migration of a break and its boundary line in the fixed field of a flash memory 303, to make it correspond, when making into main applications various application of this memory card 109, for example, storing of the digital work which should be protected, or when [that] reverse.
[0118] and a non-attesting field and an authentication field -- also in any, time and effort accompanying migration of a boundary line, such as data evacuation and migration processing, is reduced by matching a logical block and a physical block so that it may be used toward the physical block of the address near a boundary line from the physical block of the address distant from a boundary line. Moreover, such matching is separating into the translation table 1102 of authentication field 332 dedication, and the translation table 1103 of non-attesting field 331 dedication, and preparing, and it becomes easy the to realize it.
[0119] In addition, in the authentication field 332, although the logical address and a physical address had become a reverse order in the unit of a block, it is not restricted to such a unit, for example, is good in a cutting tool's unit also as a reverse order in considering as a reverse order in the unit of a sector. As

mentioned above, although the memory card of this invention was explained using the gestalt and modification of operation, this invention is not limited to these.
[0120] For example, although authentication with the memory card 109 by the procedure same whenever it emits the command for accessing the authentication field 332 of a memory card 109 was needed, you may enable it to access PC102 and a player 201 in the authentication procedure simplified depending on the class of command. For example, about a write command "SecureWrite", though it is necessary to take out neither encryption master key 323b nor media ID 341 from a memory card 109, it only succeeds in authentication of a uni directional (authentication of the device by the memory card 109) and a memory card 109 performs, it is good. The execution speed is accelerated by this about the command whose relation with protection of copyrights is not so strong.
[0121] Moreover, even if it transposes the flash memory 303 which the memory card 109 of this invention has to non-volatilized media, such as other storage media, for example, a hard disk, an optical disk, and a magneto-optic disk, it cannot be overemphasized that the pocket mold storage card in which the same protection of copyrights as this invention is possible is realized.
[0122]
[Effect of the Invention] The semi-conductor memory card concerning this invention so that clearly from the above explanation It is a semi-conductor memory card removable on electronic equipment. Rewritable nonvolatile memory, The control circuit which controls access by said electronic equipment to the authentication field and the non-attesting field which are two storage regions where it was beforehand set in said nonvolatile memory, It has the area-size modification circuit which changes the area size of said authentication field and each of said non-attesting field. Said control circuit The non-attesting field access-control section which controls access by said electronic equipment to said non-attesting field, The authentication section which tries authentication of said electronic equipment in order to verify the justification of said electronic equipment, It has the authentication field access-control section which permits access by said electronic equipment to said authentication field only when said authentication section succeeds in authentication. Said authentication field and said non-attesting field It is assigned to each field obtained by carrying out the storage region where the fixed size in said nonvolatile memory continued for 2 minutes. Said area-size modification circuit The authentication field translation table showing correspondence with the logical address and the physical address in said authentication field, The non-attesting field translation table showing correspondence with the logical address and the physical address in said non-attesting field, It has the translation table modification section which changes said authentication field translation table and said authentication field translation table according to the instruction from said electronic equipment. Said authentication field access-control section Access by said electronic equipment is controlled based on said authentication field translation table. Said non-attesting field access-control section Access by said electronic equipment is controlled based on said non-attesting field translation table. Said authentication field and said non-attesting field It is assigned to the high field and the low field of the physical address obtained by carrying out the storage region of said fixed size for 2 minutes, respectively. Said non-attesting field translation table Said authentication field translation table is characterized by matching the logical address and a physical address so that the ascending order of the logical address may turn into ascending order of a physical address, and matching the logical address and a physical address so that the ascending order of the logical address may turn into descending order of a physical address.
[0123] It can be used by storing the data in connection with protection of copyrights in an authentication field, and storing in a non-attesting field by this, the data which are not so, making a digital work and a non-work intermingled, and the semi-conductor memory card which has both applications is realized. As for said non-attesting field translation table, the logical address and a physical address are matched so that the ascending order of the logical address may turn into ascending order of a physical address, and the probability for the field near the boundary of an authentication field and a non-attesting field to be used becomes low by using said authentication field translation table for the ascending order of the logical address, since the logical address and a physical address are matched so that the ascending order of the logical address may turn into descending order of a physical address. Therefore, the probability

for processing of data evacuation, migration, etc. which are needed when the boundary is moved to occur also becomes low, and modification of area size is simplified.

[0124] Since said authentication field access-control section and said non-attesting field access-control section can be easily changed so that it may become the logical block which continued logically even if the phenomenon which two or more logical blocks which constitute the same file fragment arises, since access by said electronic equipment is controlled based on said translation table, access to the same file is accelerated.

[0125] Said authentication section generates the key data reflecting the result of authentication here, and though said authentication field access-control section is decoded by the key data by which said authentication section generated the enciphered instruction which is sent from said electronic equipment and controls access to said authentication field according to the decoded instruction, it is good. Even if the exchange with a semi-conductor memory card and electronic equipment is intercepted by this, since it is enciphered by it depending on the authentication result to which the instruction for accessing an authentication field was carried out immediately before, by it, the prevention function to unjust access to an authentication field becomes high.

[0126] Moreover, though said authentication section generates said key data from the response data generated in order to prove the challenge data transmitted to said electronic equipment in order to perform mutual recognition of said electronic equipment and a challenge response mold and to verify the justification of said electronic equipment, and self justification, it is good. The safety of the authentication field which cannot be accessed by this if such key data are not used for them, since key data have the property to be shared in both sides for the first time only when the both sides of a semi-conductor memory card and electronic equipment succeed in mutual recognition, and to change at every authentication becomes a stronger thing.

[0127] Moreover, the enciphered instruction which is sent from said electronic equipment It consists of the tag section which specifies the classification of access to said authentication field and which is not enciphered, and enciphered address part which pinpoints the field to access. Said authentication section It is good though execution control of the access of the classification specified by the tag section of said instruction is carried out to the field which decodes the address part of said instruction and is pinpointed by the decoded address using said key data.

[0128] Since only the address part of an instruction is enciphered by this, by it, the decode by the semi-conductor memory card and decode processing in which such an instruction was received become simple. Moreover, said semi-conductor memory card is equipped with the discernment data store circuit which memorizes beforehand the discernment data of the proper which can specify self in distinction from the semi-conductor memory card of further others, and though said authentication section performs mutual recognition using the discernment data stored in said discernment data store circuit, makes it dependent on said discernment data and generates said key data, it is good.

[0129] In mutual recognition, since it is exchanged in the data depending on each semi-conductor memory card by this, high safety is maintainable to decode of inaccurate mutual recognition with this. Moreover, said semi-conductor memory card may be equipped with the read-only memory circuit in which data were stored further beforehand. The function of protection of copyrights is strengthened with storing discernment data distinguishable from other semi-conductor memory cards etc. in a read-only memory, making it dependent on the discernment data, and storing a digital work by this.

[0130] Moreover, said authentication field and said non-attesting field consist of a storage region which can be written for said electronic equipment, and a read-only storage region. Said control circuit has the random number generator which generates a random number whenever it accesses further for said electronic equipment.writing data in said nonvolatile memory. Said authentication field access-control section and said non-attesting field access-control section While enciphering and writing said data in the storage region which can write [said] the obtained encryption data using said random number, it is good though said random number is written in said read-only storage region matched with said encryption data.

[0131] Since it becomes possible to detect such an action by inspecting adjustment with the random

number stored in the read-only storage region even if the unjust alteration to the storage region which can be written etc. is performed by this, safer data logging is realized. Said control circuit may have the code decode section which decrypts the data read from said authentication field and said non-attesting field while enciphering further the data which should be written in said authentication field and said non-attesting field. A semi-conductor memory card is destroyed and this enables it to be equal to the unjust attack of reading the memory content of an authentication field and a non-attesting field directly.
[0132] Moreover, said nonvolatile memory is a flash memory, and said control circuit may pinpoint further the field which is not eliminated [which exists in said authentication field and said authentication field] according to the instruction from said electronic equipment, and may have the non-eliminated list read-out section which sends the information which shows the field to said electronic equipment. By this, since electronic equipment can know a non-eliminated field and can eliminate the field in advance in advance of rewriting of a flash memory, high-speed rewriting of it is attained.
[0133] Moreover, the user key storage section for said authentication section to require the user key which is the information on a proper of the user from the user who uses electronic equipment for authentication, and for said control circuit memorize said user key further, The identification information storage section for memorizing the identification information which can specify the electronic equipment which succeeded in authentication by said authentication section, If authentication by said authentication section is started, identification information will be acquired from the electronic equipment. When the identification information inspects whether it is already stored in said identification information storage section and is already stored in it, you may have the user key demand prohibition section in which the demand of the user key by said authentication section is forbidden.
[0134] Since the time and effort that the input of a password or personal data is required whenever it uses it for a semi-conductor memory card by this, connecting is avoided, generating of the fault that personal data are intercepted and used unjustly is suppressed. The read-out equipment concerning this invention is read-out equipment which reads the digital work stored in the above-mentioned semi-conductor memory card. Said semi-conductor memory card While the digital work is stored in the non-attesting field, the count which permits read-out of said digital work is beforehand stored in an authentication field. Said read-out equipment A decision means to judge whether the count stored in said authentication field is read, and read-out is permitted by the count in case the digital work stored in said non-attesting field is read, Only when the permission is granted, while reading said digital work from said non-attesting field, it is characterized by having the playback means which subtracts said read count and is returned to said authentication field.
[0135] By this, it becomes possible to restrict the count of read-out of the digital work stored in the semi-conductor memory card, and becomes applicable to the charged rental of a music content etc. Moreover, the read-out equipment concerning this invention is read-out equipment which reads the digital work stored in the above-mentioned semi-conductor memory card, and is reproduced to an analog signal. While the digital work refreshable to an analog signal is stored in the non-attesting field, said semi-conductor memory card The count which permits the digital output by said electronic equipment of said digital work is beforehand stored in an authentication field. Said read-out equipment A playback means to read the digital work stored in said non-attesting field, and to reproduce to an analog signal, Only when the permission is granted with a decision means to judge whether the count stored in said authentication field is read, and the digital output is permitted by the count, while outputting said digital work outside with a digital signal It is characterized by having the digital output means which subtracts said read count and is returned to said authentication field.
[0136] It becomes possible to restrict the count of the digital copy of the digital work stored in the semi-conductor memory card by this, and the fine protection of copyrights of the grain in alignment with an intention of a copyright person becomes possible. Thus, this invention is a semi-conductor memory card which has the flexible function which combines both the application as a record medium of a digital work, and the application as an auxiliary storage unit of a computer, the effectiveness of securing healthy circulation of the digital work accompanying an electronic music distribution especially is done so, and the practical value is very large.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] They are a personal computer concerning the electronic music distribution in the gestalt of operation of this invention, and drawing showing the appearance of a removable semi-conductor memory card in the PC.
[Drawing 2] It is drawing showing the appearance of the player of the pocket mold which uses this semi-conductor memory card as a record medium.
[Drawing 3] It is the block diagram showing the hardware configuration of this personal computer.
[Drawing 4] It is the block diagram showing the hardware configuration of this player.
[Drawing 5] It is drawing showing the appearance and hardware configuration of this semi-conductor memory card.
[Drawing 6] It is drawing showing the class of storage region of this semi-conductor memory card seen from this personal computer or this player.
[Drawing 7] (a) shows the Ruhr in access to each field, it is drawing showing the limit at the time of this personal computer and this player accessing each field of this semi-conductor memory card, and the gestalt of a command, and (c) is [(b) shows the Ruhr in modification of the size of each field, and] the conceptual diagram showing the field of this semi-conductor memory card.
[Drawing 8] It is the flow Fig. showing the actuation in which this personal computer (and this player) writes contents, such as music data, in this semi-conductor memory card.
[Drawing 9] It is the flow Fig. showing the actuation which reads contents, such as music data, from this semi-conductor memory card, and is reproduced by this player (and this personal computer).
[Drawing 10] This player (and this personal computer) is the flow Fig. showing the actuation which was stored in the authentication field of this semi-conductor memory card, and which reads and operates a count.
[Drawing 11] This player (and this personal computer) is the flow Fig. showing the actuation which operates the count of digital output authorization stored in the authentication field of this semi-conductor memory card.
[Drawing 12] It is drawing showing DS common to the authentication field and the non-attesting field of this semi-conductor memory card, and the flow of the R/W processing corresponding to the DS.
[Drawing 13] It is drawing showing signs that correspondence with the logical address of this semi-conductor memory card and a physical address is changed, and the translation table corresponding to [(a)] (a) in (c) and (d) show the translation table corresponding to (b) corresponding to the correspondence relation after modification in the correspondence relation before modification, and (b).
[Drawing 14] (b) shows the non-eliminated list in the condition, it is drawing explaining the function about the non-eliminated block which this semi-conductor memory card has, and (d) is [(a) shows the busy condition of a logical block and a physical block and / (c) is the flow Fig. showing actuation in case PC102 and a player 201 eliminate a block in advance using a non-eliminated list command and an elimination command, and] the table showing the busy condition of a logical block.
[Drawing 15] It is drawing showing the communication link sequence and the main components

between this player for authentication, and this semi-conductor memory card.
[Drawing 16] It is the communication link sequence diagram showing the authentication procedure of the this semi-conductor memory card and external instrument concerning the modification of this invention.
[Drawing 17] It is the communication link sequence diagram showing the detailed procedure of mutual recognition shown in drawing 16 .
[Drawing 18] It is drawing showing the condition before modification in modification of the boundary line of the authentication field of this semi-conductor memory card, and a non-attesting field, and (a) is a memory map in which the configuration of the physical block of a flash memory is shown, (b) shows the translation table only for non-attesting fields, and (c) shows the translation table only for authentication fields.
[Drawing 19] It is drawing showing the condition after modification in modification of the boundary line of the authentication field of this semi-conductor memory card, and a non-attesting field, and (a) is a memory map in which the configuration of the physical block of a flash memory is shown, (b) shows the translation table only for non-attesting fields, and (c) shows the translation table only for authentication fields.
[Description of Notations]
101 Communication Line
102 PC
103 Display
104 Keyboard
105 Memory Card Writer Insertion Opening
106 Loudspeaker
107 Memory Card Writer
108 Memory Card Insertion Opening
109 Memory Card
110 CPU
111 ROM
112 RAM
113 Communication Link Port
114 Internal Bus
117 Descrambler
118 AAC Decoder
119 D/A Converter
120 Hard Disk
201 Player
202 Manual Operation Button
203 Liquid Crystal Display Section
204 Analog Output Terminal
205 Digital Output Terminal
206 Memory Card Insertion Opening
208 Headphone
210 CPU
211 ROM
212 RAM
213 Communication Link Port
214 Internal Bus
215 Card I/F Section
216 Authentication Circuit
217 Descrambler
218 AAC Decoder

219 D/A Converter
220 AAC Encoder
221 A/D Converter
222 Scrambler
223 Analog Input Terminal
224 Loudspeaker
302 Control IC
303 Flash Memory
304 ROM (Special Field)
321 Authentication Section
322 Command Judging Control Section
323 Master Key Storage Section
323a Master key
323b Encryption master key
324 Special Field Access-Control Section
325 Authentication Field Access-Control Section
326 Non-Attesting Field Access-Control Section
327 Code and Decryption Circuit
331 Non-Attesting Field
332 Authentication Field
341 Media ID
342 Manufacture Manufacture Name
343 Secure Media ID
425 Cryptographic Key
426 Encryption Contents
427 User Data
501 Alternative Block Field
812 Count of Read-out
913 Count of Digital Output Authorization
1003 Random Number Generator
1004 Sector
1005 Extended Partition
1006 ECC Data
1007 the Time -- Strange Field
1101 Translation Table
1102 Translation Table Only for Authentication Fields
1103 Translation Table Only for Non-Attesting Fields
1203 Non-Eliminated List
1301 Master Key
1302 Device-dependent [ID]
1310 Device-dependent ID Group Storage Region
1311 User Key Storage Region

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－233795
（Ｐ2003－233795Ａ）
(43)公開日　平成15年８月22日(2003.8.22)

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード'（参考）
Ｇ０６Ｋ　19/10		Ｃ０６Ｆ　12/14	３１０Ｈ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３１０		３２０Ｂ	５Ｂ０３５
	３２０		３２０Ｆ	５Ｂ０５８
		Ｇ０６Ｋ　17/00	Ｔ	５Ｊ１０４
Ｇ０６Ｋ　17/00		Ｃ０９Ｃ　1/00	６４０Ｅ	

審査請求　未請求　請求項の数12　ＯＬ　（全 27 頁）　最終頁に続く

(21)出願番号　特願2002－346019(Ｐ2002－346019)
(62)分割の表示　特願平11－374788の分割
(22)出願日　平成11年12月28日(1999.12.28)

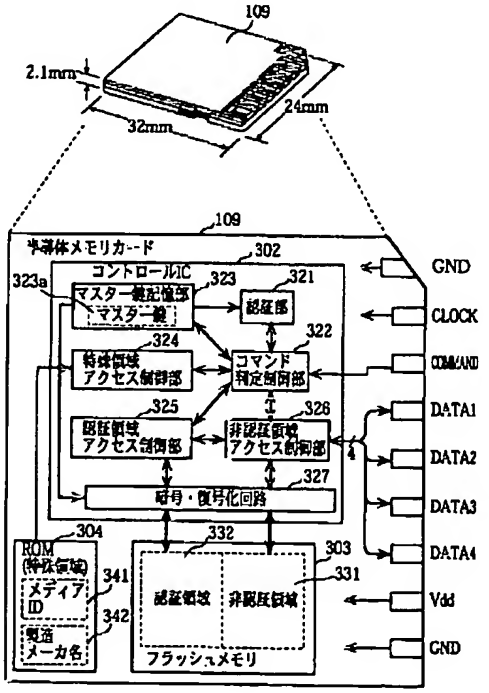
(31)優先権主張番号　特願平11－119441
(32)優先日　平成11年４月27日(1999.4.27)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　廣田　照人
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　半導体メモリカード及び読み出し装置

(57)【要約】
【課題】　デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の記憶媒体としても用いることが可能な半導体メモリカードを提供する。
【解決手段】　コントロールＩＣ３０２とフラッシュメモリ３０３とＲＯＭ３０４とからなり、ＲＯＭ３０４は、このカードに固有のメディアＩＤ３４１等を保持し、フラッシュメモリ３０３は、外部機器の認証に成功した場合にのみその外部機器にアクセスを許可する認証領域３３２と認証の結果に拘わらずアクセスを許可する非認証領域３３１とを有し、コントロールＩＣ３０２は、外部機器による認証領域３３２及び非認証領域３３１へのアクセスを制御する制御部３２５、３２６及び外部機器との相互認証を実行する認証部３２１等を有する。



【特許請求の範囲】

【請求項１】　電子機器に着脱可能な半導体メモリカードであって、
書き換え可能な不揮発メモリと、
前記不揮発メモリ内の予め定められた２つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路と、
前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、
前記制御回路は、
前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、
前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、
前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、
前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を２分して得られる各領域に割り当てられ、
前記領域サイズ変更回路は、
前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、
前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、
前記電子機器からの命令に従って前記認証領域変換テーブル及び前記認証領域変換テーブルを変更する変換テーブル変更部とを有し、
前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、
前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、
前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を２分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、
前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、
前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられていることを特徴とする半導体メモリカード。

【請求項２】　前記認証部は、認証の結果を反映した鍵データを生成し、
前記認証領域アクセス制御部は、前記電子機器から送られてくる暗号化された命令を前記認証部が生成した鍵データで復号し、復号された命令に従って前記認証領域へのアクセスを制御することを特徴とする請求項１記載の半導体メモリカード。

【請求項３】　前記認証部は、前記電子機器とチャレンジ・レスポンス型の相互認証を行い、前記電子機器の正当性を検証するために前記電子機器に送信したチャレンジデータと自己の正当性を証明するために生成したレスポンスデータとから前記鍵データを生成することを特徴とする請求項２記載の半導体メモリカード。

【請求項４】　前記電子機器から送られてくる暗号化された命令は、前記認証領域へのアクセスの種別を特定する暗号化されていないタグ部と、アクセスする領域を特定する暗号化されたアドレス部とからなり、
前記認証部は、前記鍵データを用いて、前記命令のアドレス部を復号し、復号されたアドレスによって特定される領域に対して、前記命令のタグ部によって特定される種別のアクセスを実行制御することを特徴とする請求項３記載の半導体メモリカード。

【請求項５】　前記半導体メモリカードはさらに、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データを予め記憶する識別データ記憶回路を備え、
前記認証部は、前記識別データ記憶回路に格納された識別データを用いて相互認証を行い、前記識別データに依存させて前記鍵データを生成することを特徴とする請求項４記載の半導体メモリカード。

【請求項６】　前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備えることを特徴とする請求項１記載の半導体メモリカード。

【請求項７】　前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、
前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、
前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データに対応づけられた前記読み出し専用の記憶領域に書き込むことを特徴とする請求項１記載の半導体メモリカード。

【請求項８】　前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有することを特徴とする請求項１記載の半導体メモリカード。

【請求項９】　前記不揮発メモリは、フラッシュメモリであり、
前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有することを特徴とする請求項１記載の半導体メモリカード。

【請求項１０】　前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、
前記制御回路はさらに、
前記ユーザキーを記憶しておくためのユーザキー記憶部と、
前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、
前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有することを特徴とする請求項１記載の半導体メモリカード。
【請求項１１】　請求項１記載の半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、
前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、
前記読み出し装置は、
前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているか否か判断する判断手段と、
許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする読み出し装置。
【請求項１２】　請求項１記載の半導体メモリカードに格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、
前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、
前記読み出し装置は、
前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、
前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているか否か判断する判断手段と、
許可されている場合にのみ前記デジタル著作物をデジタル信号のまま外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする読み出し装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタル著作物等を記憶するための半導体メモリカード及びその読み出し装置に関し、特に、デジタル著作物の著作権保護に好適な半導体メモリカード及び読み出し装置に関する。
【０００２】
【従来の技術】近年、マルチメディア・ネットワーク技術の発展により、音楽コンテンツ等のデジタル著作物がインターネット等の通信ネットワークを通じて配信されるようになり、自宅に居ながらにして世界中の音楽等に接することが可能となってきた。例えば、パーソナルコンピュータ（以下、「ＰＣ」という。）で音楽コンテンツをダウンロードした後、ＰＣに装着された半導体メモリカードに格納しておくことで、必要に応じて音楽を再生し楽しむことができる。また、このようにして音楽コンテンツを格納した半導体メモリカードをＰＣから取り出して携帯型音楽再生装置に装着しておくことで、歩きながら音楽を聴くこともできる。このような半導体メモリカードは、フラッシュメモリ等の不揮発性で、かつ、大きな記憶容量の半導体メモリを内蔵した小型軽量の便利なカードである。
【０００３】ところで、このような電子音楽配信において、半導体メモリカードにデジタル著作物を記憶する場合、不正なコピーを防止するために、鍵等を用いてコンテンツを暗号化しておく必要がある。また、ＰＣ等に標準添付されて広く出回っているファイル管理ソフトウェアによっては他の記憶媒体等にコピーすることができないようにしておく必要もある。
【０００４】このような不正なコピーを防止する方法として、半導体メモリカードへのアクセスを専用のソフトウェアでのみ可能とする方策が考えられる。例えば、ＰＣと半導体メモリカード間での認証が成功した時にのみ半導体メモリカードへのアクセスを許可することとし、専用のソフトウェアがないためにその認証に成功することができない場合には半導体メモリカードへのアクセスが禁止されるとする方法が考えられる。
【０００５】
【発明が解決しようとする課題】しかしながら、ＰＣが半導体メモリカードにアクセスするのに常に専用のソフトウェアが必要とされるのでは、そのような専用のソフトウェアを所有していない不特定のユーザと半導体メモリカードを介して自由にデータ交換し合うことが不可能となってしまう。そのために、フラッシュＡＴＡやコンパクトフラッシュ（登録商標）等の従来の半導体メモリカードが有していた利便性、即ち、専用のソフトウェアを必要とすることなくＰＣに標準添付されているファイル管理ソフトウェアでアクセスすることができるという利便性が得られなくなってしまう。
【０００６】つまり、専用のソフトウェアでのみアクセス可能な半導体メモリカードは、著作権保護の機能を有する点でデジタル著作物の記憶媒体としては適しているが、汎用的な使用が困難であるために一般的なコンピュ

ータシステムにおける補助記憶装置として使用することができないという問題点がある。そこで、本発明は、このような問題点に鑑みてなされたものであり、デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の記憶媒体としても用いることが可能な半導体メモリカード及びその読み出し装置を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明に係る半導体メモリカードは、電子機器に着脱可能な半導体メモリカードであって、書き換え可能な不揮発メモリと、前記不揮発メモリ内の予め定められた2つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路と、前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、前記制御回路は、前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を2分して得られる各領域に割り当てられ、前記領域サイズ変更回路は、前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、前記電子機器からの命令に従って前記認証領域変換テーブル及び前記認証領域変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を2分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられていることを特徴とする。

【0008】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。図1は、通信ネットワークを介して音楽コンテンツ等のデジタル著作物をダウンロードするPCと、そのPCに着脱可能な半導体メモリカード（以下、単に「メモリカード」という。）の外観を示す図である。

【0009】PC102は、ディスプレイ103、キーボード104及びスピーカ106等を備え、内蔵するモデムによって通信回線101に接続されている。そして、このPC102が有するPCMCIA等のカードスロット（メモリカードライタ挿入口105）にはメモリカードライタ107が挿入されている。メモリカードライタ107は、PC102とメモリカード109とを電気的に接続するアダプタであり、そのメモリカード挿入口108にメモリカード109が装着されている。

【0010】このようなシステムを用いることによって、ユーザは、以下の手順を経ることで、インターネット上にあるコンテンツプロバイダが提供する音楽データを取得することができる。まず、ユーザは、所望の音楽コンテンツを、通信回線101を通じて、PC102内部のハードディスクにダウンロードする。音楽データは暗号化されており、そのままではPC102では再生することはできない。

【0011】再生するためには、ダウンロード元のコンテンツプロバイダへクレジットカード等を用いてお金を払っておく必要がある。支払いを済ますと、コンテンツプロバイダよりパスワードと権利情報を入手することができる。パスワードは、暗号化された音楽データを解除するのに必要な鍵データである。権利情報は、PCでの再生可能回数や、メモリカードへの書き込み可能回数、再生可能な期間を示す再生期限等のユーザに許可された再生条件を示す情報である。

【0012】パスワードと権利情報を取得したユーザは、PC102のスピーカ106から音楽を再生出力させる場合には、著作権保護機能が付いた専用のアプリケーションプログラム（以下、このプログラムを単に「アプリケーション」という。）に対して、入手したパスワードをキーボード104から入力する。すると、そのアプリケーションは、権利情報を確認した後に、暗号化された音楽データをパスワードを用いて復号しながらスピーカ106を通じて音声として再生出力する。

【0013】また、権利情報としてメモリカードへの書き込みが許可されている場合には、そのアプリケーションは、暗号化された音楽データ、パスワード、権利情報をメモリカード109に書き込むことができる。図2は、このメモリカード109を記録媒体とする携帯型の録音再生装置（以下、「プレーヤ」という。）201の外観を示す図である。

【0014】プレーヤ201の上面には、液晶表示部203と操作ボタン202が設けられ、手前側面には、メモリカード109を着脱するためのメモリカード挿入口206及びPC102等と接続するためのUSB等の通信ポート213が設けられ、右側面には、アナログ出力端子204、デジタル出力端子205及びアナログ入力端子223等が設けられている。

【0015】プレーヤ201は、メモリカード109に格納された音楽データ、パスワード、権利情報に基づいて、再生が許可されている状態にあるならば、その音楽データを読み出して復号した後にアナログ信号に変換し、アナログ出力端子204に接続されたヘッドフォン208を通じて音声として出力したり、再生中の音楽データをデジタルデータのままデジタル出力端子205に出力したりする。

【0016】また、このプレーヤ201は、マイク等を介してアナログ入力端子223から入力されるアナログの音声信号をデジタルデータに変換してメモリカード109に記録したり、通信ポート213を介して接続されたPC102と通信することによって、そのPC102によってダウンロードされた音楽データ、パスワード及び権利情報をメモリカード109に記録することができる。つまり、このプレーヤ201は、メモリカード109への音楽データの記録及びメモリカード109に記録された音楽データの再生に関して、図1に示されたPC102及びメモリカードライタ107に置き換わる機能を有する。

【0017】図3は、PC102のハードウェア構成を示すブロック図である。PC102は、CPU110、デバイス鍵111aや制御プログラム111b等を予め記憶しているROM111、RAM112、ディスプレイ103、通信回線101と接続するためのモデムポートやプレーヤ201と接続するためのUSB等を備える通信ポート113、キーボード104、内部バス114、メモリカード109と内部バス214とを接続するメモリカードライタ107、メモリカード109から読み出された暗号化音楽データを復号するデスクランブラ1117、復号された音楽データを伸張するMPEG2-AAC（ISO13818-7）に準拠したAACデコーダ118、伸張されたデジタル音楽データをアナログ音声信号に変換するD/Aコンバータ119、スピーカ106及びファイル管理ソフトウェアやアプリケーションを格納しているハードディスク120等から構成される。

【0018】このPC102は、ハードディスク120に格納されたファイル管理ソフトウェアを実行することで、メモリカード109をハードディスクのように独立したファイルシステム（ISO9293等）を有する補助記憶装置として用いることができるだけでなく、ハードディスク120に格納された上述の専用アプリケーションを実行することで、通信ポート113のモデム等を介して通信回線101から音楽コンテンツ等をダウンロードしたり、メモリカード109との相互認証を行なった後に音楽コンテンツ等をメモリカード109に格納したり、メモリカード109に格納されている音楽コンテンツ等を読み出してスピーカ106に再生出力したりする。

【0019】なお、ROM111に格納されたデバイス鍵111aは、このPC102に固有の秘密鍵であり、後述するように、相互認証等に用いられる。図4は、プレーヤ201のハードウェア構成を示すブロック図である。プレーヤ201は、CPU210、デバイス鍵211aや制御プログラム211b等を予め記憶しているROM211、RAM212、液晶表示部203、PC102等と接続するためのUSB等の通信ポート213、操作ボタン202、内部バス214、メモリカード109と内部バス214とを接続するカードI/F部215、メモリカード109との相互認証を実行する認証回路216、メモリカード109から読み出された暗号化音楽データを復号するデスクランブラ217、復号された音楽データ伸張するMPEG2-AAC（ISO13818-7）に準拠したAACデコーダ218、伸張されたデジタル音楽データをアナログ音声信号に変換するD/Aコンバータ219、スピーカ224、アナログ入力端子223から入力されたアナログ音楽信号をデジタル音楽データに変換をするA/Dコンバータ221、そのデジタル音楽データをMPEG2-AAC（ISO13818-7）に準拠して圧縮符号化するAACエンコーダ220、圧縮符号化された音楽データを暗号化するスクランブラ222、アナログ出力端子204、デジタル出力端子205及びアナログ入力端子223から構成される。

【0020】このプレーヤ201は、ROM211に格納された制御プログラム211bをRAM212にロードしCPU210に実行させることで、メモリカード109に格納されている音楽コンテンツ等を読み出してスピーカ224に再生出力したり、アナログ入力端子223や通信ポート213を経て入力された音楽コンテンツ等をメモリカード109に格納したりする。つまり、通常のプレーヤと同様に、個人的に音楽を録音したり再生したりして楽しむことができるだけでなく、PC102によりダウンロードされた電子音楽配信に係る（著作権保護が必要とされる）音楽コンテンツの記録・再生もできる。

【0021】図5は、メモリカード109の外観及びハードウェア構成を示す図である。メモリカード109は、何度も繰り返して書き込みが行える書き換え可能な不揮発性メモリを内臓しており、その記憶容量は64MBであり、外部から3．3Vの電源とクロック信号の供給を受けて動作する。また、メモリカード109は、厚さ2．1mm、縦32mm、横24mmの直方体形状で、その側面に書き込み防止スイッチ（ライトプロテクトSW）を有し、9ピンの接続端子によって電気的に外部機器と接続される。

【0022】このメモリカード109は、3つのICチップ（コントロールIC302、フラッシュメモリ303、ROM304）を内蔵している。フラッシュメモリ

３０３は、一括消去型の書き換え可能な不揮発メモリであり、論理的な記憶領域として、正当な機器であると認証することができた機器だけに対してアクセスを許可する記憶領域である認証領域３３２と、そのような認証を必要とすることなくアクセスを許可する記憶領域である非認証領域３３１等を有する。ここでは、認証領域３３２は、著作権保護に関わる重要なデータを格納するために用いられ、非認証領域３３１は、一般的なコンピュータシステムにおける補助記憶装置として用いられる。なお、これら２つの記憶領域は、フラッシュメモリ３０３上の一定のアドレスを境界として区分されている。

【００２３】ＲＯＭ３０４は、特殊領域と呼ばれる読み出し専用の記憶領域を有し、このメモリカード１０９に固有の識別情報であるメディアＩＤ３４１やこのメモリカード１０９の製造メーカ名３４２等の情報を予め保持している。なお、メディアＩＤ３４１は、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データであり、ここでは、機器間の相互認証に用いられ、認証領域３３２への不正なアクセスを防止するために使用される。

【００２４】コントロールＩＣ３０２は、アクティブ素子（論理ゲート等）からなる制御回路であり、認証部３２１、コマンド判定制御部３２２、マスター鍵記憶部３２３、特殊領域アクセス制御部３２４、認証領域アクセス制御部３２５、非認証領域アクセス制御部３２６及び暗号・復号化回路３２７等を有する。認証部３２１は、このメモリカード１０９にアクセスしようとする相手機器とチャレンジ・レスポンス型の相互認証を行う回路であり、乱数発生器や暗号器等を有し、その暗号器と同一の暗号器を相手機器が有しているか否かを検出することによって、相手機器の正当性を認証する。なお、チャレンジ・レスポンス型の相互認証とは、相手機器の正当性を検証するためにチャレンジデータを相手機器に送り、それに対して相手機器において自己の正当性を証明する処理が施こされて生成されたレスポンスデータを相手機器から受け取り、それらチャレンジデータとレスポンスデータとを比較することで相手機器を認証することができるか否かを判断するという認証ステップを、双方の機器が相互に行うことである。

【００２５】コマンド判定制御部３２２は、コマンドピンを介して入力されたコマンド（このメモリカード１０９への命令）の種類を判定し実行するデコード回路や制御回路からなるコントローラであり、入力されたコマンドの種類に応じて、各種構成要素３２１～３２７を制御する。コマンドには、フラッシュメモリ３０３のデータを読み・書き・消去するコマンドだけでなく、フラッシュメモリ３０３を制御するためのコマンド（アドレス空間や未消去データに関するコマンド等）も含まれる。

【００２６】例えば、データの読み書きに関しては、認証領域３３２にアクセスするためのコマンド「SecureRead address count」、「SecureWrite address count」や、非認証領域３３１にアクセスするためのコマンド「Read address count」、「Write address count」等が定義されている。ここで、「address」は、読み書きの対象となる一連のセクタ群の最初のセクタの番号であり、「count」は、読み書きする合計セクタ数を示す。また、セクタは、メモリカード１０９に対してデータを読み書きする際の単位であり、ここでは、５１２バイトである。

【００２７】マスター鍵記憶部３２３は、相互認証の際に相手機器が用いたり、フラッシュメモリ３０３内のデータを保護するために用いられるマスター鍵３２３ａを予め記憶している。特殊領域アクセス制御部３２４は、特殊領域（ＲＯＭ３０４）に格納されたメディアＩＤ３４１等を読み出す回路である。

【００２８】認証領域アクセス制御部３２５及び非認証領域アクセス制御部３２６は、それぞれ、フラッシュメモリ３０３の認証領域３３２及び非認証領域３３１へのデータ書き込み及び読み出しを実行する回路であり、４本のデータピンを介して外部機器（ＰＣ１０２やプレーヤ２０１等）との間でデータを送受信する。なお、これらアクセス制御部３２５、３２６は、内部に１ブロック分のバッファメモリを有し、論理的には（外部機器とのコマンド上でのアクセスは）セクタを単位として入出力するが、フラッシュメモリ３０３の内容を書き換えるときには、ブロック（３２個のセクタ、１６Ｋバイト）を単位として入出力する。具体的には、ある１個のセクタデータを書き換える場合には、フラッシュメモリ３０３から該当するブロックをバッファメモリに読み出し、そのブロックを一括消去するとともに、バッファメモリ中の該当セクタを書き換えた後に、そのブロックをバッファメモリからフラッシュメモリ３０３に書き戻す。

【００２９】暗号・復号化回路３２７は、認証領域アクセス制御部３２５及び非認証領域アクセス制御部３２６による制御の下で、マスター鍵記憶部３２３に格納されたマスター鍵３２３ａを用いて暗号化及び復号化を行う回路であり、フラッシュメモリ３０３にデータを書き込む際にそのデータを暗号化して書き込み、フラッシュメモリ３０３からデータを読み出した際にそのデータを復号化する。これは、不正なユーザがこのメモリカード１０９を分解してフラッシュメモリ３０３の内容を直接解析し、認証領域３３２に格納されたパスワードを盗む等の不正行為を防止するためである。

【００３０】なお、コントロールＩＣ３０２は、これら主要な構成要素３２１～３２７の他に、クロックピンから供給されるクロック信号に同期した内部クロック信号を生成し各構成要素に供給する同期回路や、揮発性の記憶領域及び不揮発性の記憶領域等を有する。また、特殊領域（ＲＯＭ３０４）に格納されている情報の改ざんを防止するために、そのＲＯＭ３０４をコントロールＩＣ

３０２の中に内蔵させたり、それらの情報をフラッシュメモリ３０３に格納し、外部から書き込みできないように特殊領域アクセス制御部３２４が制限をかけてもよい。そのときに、暗号・復号化回路３２７で暗号化したデータを格納することとしてもよい。

【００３１】図6は、ＰＣ１０２やプレーヤ２０１から見たメモリカード１０９の記憶領域の種類を示す図である。メモリカード１０９が有する記憶領域は、大きく分けて、特殊領域３０４と認証領域３３２と非認証領域３３１の3つの領域である。特殊領域３０４は読み出し専用の領域で、この中のデータに対しては、専用コマンドを用いて読み出しを行う。認証領域３３２は、ＰＣ１０２又はプレーヤ２０１とメモリカード１０９との間で認証が成功した時にのみ読み書きができる領域で、この領域へのアクセスについては暗号化されたコマンドを用いる。非認証領域３３１は、ＡＴＡやＳＣＳＩ等の公開されたコマンドでアクセスできる、即ち、認証せずに読み書きできる領域である。従って、非認証領域３３１に対しては、フラッシュＡＴＡやコンパクトフラッシュ（登録商標）と同じように、ＰＣ１０２上のファイル管理ソフトウェアでデータの読み書きが可能である。

【００３２】3つの記憶領域には、以下の情報を格納することとし、これによって、一般的なＰＣの補助記憶装置として機能と、電子音楽配信に係る音楽データに対する著作権保護の機能とを提供している。つまり、非認証領域３３１には、著作権保護の対象となる音楽データが暗号化された暗号化コンテンツ４２６や、著作権保護とは無関係な一般的なデータであるユーザデータ４２７等が格納される。認証領域３３２には、非認証領域３３１に格納された暗号化コンテンツ４２６を復号するための秘密鍵となる暗号化キー４２５が格納される。そして、特殊領域３０４には、認証領域３３２にアクセスするために必要とされる情報であるメディアＩＤ３４１が格納されている。

【００３３】ＰＣ１０２やプレーヤ２０１は、まず、装着されたメモリカード１０９の特殊領域３０４に格納されたメディアＩＤ３４１を読み出し、それを用いて認証領域３３２に格納された暗号化キー４２５、権利情報を取り出す。それら暗号化キー４２５や権利情報によって再生が許可されていれば、非認証領域３３１にある暗号化コンテンツ４２６を読み出し、暗号化キー４２５で復号しながら、再生を行うことができる。

【００３４】もし、あるユーザが不正に入手した音楽データだけをＰＣ１０２等でメモリカード１０９の非認証領域３３１に書き込み、そのようなメモリカード１０９をプレーヤ２０１に装着して再生しようとしたとする。しかし、そのメモリカード１０９の非認証領域３３１に音楽データが格納されているものの、認証領域３３２に対応する暗号化キー４２５や権利情報が存在しないために、そのプレーヤ２０１は、その音楽データを再生することができない。これによって、正規の暗号化キーや権利情報を伴わないで音楽コンテンツだけをメモリカード１０９に複製しても、その音楽コンテンツは再生されないので、デジタル著作物の不正な複製が防止される。

【００３５】図7は、ＰＣ１０２やプレーヤ２０１がメモリカード１０９の各領域にアクセスする際の制限やコマンドの形態を示す図であり、（ａ）は各領域へのアクセスにおけるルールを示し、（ｂ）は各領域のサイズの変更におけるルールを示し、（ｃ）はメモリカード１０９の領域を示す概念図である。特殊領域３０４は、読み出し専用の領域であり、認証せずに専用コマンドでアクセスできる。この特殊領域３０４に格納されたメディアＩＤ３４１は、認証領域３３２にアクセスするための暗号化コマンドの生成や復号に用いられる。つまり、ＰＣ１０２やプレーヤ２０１は、このメディアＩＤ３４１を読み出し、これを用いて認証領域３３２にアクセスするコマンドを暗号化し、メモリカード１０９に送る。一方、その暗号化コマンドを受けたメモリカード１０９は、メディアＩＤ３４１を用いて、その暗号化コマンドを復号し、解釈して実行する。

【００３６】認証領域３３２は、ＰＣ１０２やプレーヤ２０１等のメモリカード１０９にアクセスする装置とメモリカード１０９との間で認証が成功した時にのみアクセスが可能となる領域であり、その大きさは（ＹＹＹＹ＋１）個のセクタに相当する。つまり、この認証領域３３２は、論理的には、第0～ＹＹＹＹのセクタで構成され、物理的には、フラッシュメモリ３０３の第ＸＸＸＸ～第（ＸＸＸＸ＋ＹＹＹＹ）のセクタアドレスを有するセクタから構成される。なお、セクタアドレスとは、フラッシュメモリ３０３を構成する全てのセクタそれぞれに対してユニークに付された一連の番号のことである。

【００３７】非認証領域３３１は、認証せずにＡＴＡやＳＣＳＩ等の標準コマンドでアクセスすることが可能で、その大きさはＸＸＸＸ個のセクタに相当する。つまり、この非認証領域３３１は、論理的にも物理的にも第0～（ＸＸＸＸ－１）のセクタで構成される。なお、フラッシュメモリ３０３には、認証領域３３２や非認証領域３３１に生じた欠陥ブロック（正常に読み書きできない不良の記憶領域を有するブロック）を代替するための交替ブロックの集まりからなる代替ブロック領域５０１が予め割り当てられることがある。

【００３８】また、特殊領域３０４は認証なしでアクセスできるとしたが、不正なユーザからの解析を防ぐために、認証を行ってからでないとアクセスできないとしてもよいし、特殊領域３０４にアクセスするコマンドを暗号化してもよい。次に、図7（ｂ）及び（ｃ）を用いて、認証領域３３２と非認証領域３３１それぞれの領域サイズを変更する方法について説明する。

【００３９】フラッシュメモリ３０３に設けられる認証領域３３２と非認証領域３３１との合計の記憶容量は、

フラッシュメモリ３０３の全記憶領域から代替ブロック領域５０１等を除いた固定値、即ち、（ＸＸＸＸ＋ＹＹＹＹ＋１）個のセクタ分であるが、それぞれの大きさは、境界アドレスＸＸＸＸの値を変更することで、可変となっている。

【００４０】領域の大きさを変更するためには、初めに認証を行う。これは、ＰＣのユーザに広く開放されている標準プログラムや不正なアクセスを行うソフト等を用いて簡単に大きさを変更することができないようにするためである。認証を行った後は、領域変更の専用コマンドで、非認証領域３３１の大きさ（新たなセクタ数ＸＸＸＸ）をメモリカード１０９に送る。

【００４１】メモリカード１０９は、その領域変更コマンドを受け取ると、その値ＸＸＸＸをメモリカード１０９内の不揮発な作業領域等に保存し、以降のアクセスにおいては、その値を新たな境界アドレスとして、認証領域３３２及び非認証領域３３１へのアクセス制御を実行する。つまり、フラッシュメモリ３０３上の物理的な第０～ＸＸＸＸのセクタを非認証領域３３１に割り当てるとともに、第ＸＸＸＸ～（ＸＸＸＸ＋ＹＹＹＹ）番目のセクタを認証領域３３２に割り当てる。そして、そのような新たなメモリマッピングに基づいて、アクセス制御部３２５及び３２６は、論理アドレスと物理アドレスとを変換したり、領域を越えるアクセス違反の発生を監視したりする。なお、論理アドレスとは、外部機器からメモリカード１０９を見た場合の（コマンド上での）データ空間におけるアドレスであり、物理アドレスとは、メモリカード１０９のフラッシュメモリ３０３が有するデータ空間におけるアドレスである。

【００４２】ここで、もし、境界アドレスを小さくすることにより、認証領域３３２のサイズを大きくした場合には、変更前との論理的な互換性を維持するために、認証領域３３２に格納されていた全てのデータを移動させる等の手当てが必要となる。そのためには、例えば、境界アドレスの移動量だけアドレスの下位方向に全データを移動（複写）させ、新たな境界アドレスから始まる論理アドレスに新たな物理アドレスが対応するように対応関係を変更すればよい。これによって、認証領域３３２に格納されていたデータの論理アドレスを維持したまま、そのデータ空間が拡大される。

【００４３】なお、領域変更のための専用コマンドについても、不正なアクセスを防止する観点から、コマンドを暗号化して用いることとしてもよい。図８は、音楽データ等のコンテンツをＰＣ１０２（及びプレーヤ２０１）がメモリカード１０９に書き込む動作を示すフロー図である。ここでは、ＰＣ１０２がメモリカード１０９へ書き込む場合（Ｓ６０１）を説明する。

【００４４】（１）ＰＣ１０２は、デバイス鍵１１１ａ等を用いて、メモリカード１０９の認証部３２１とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモリカード１０９からマスター鍵３２３ａを取り出す（Ｓ６０２）。

（２）次に、専用コマンドを用いて、メモリカード１０９の特殊領域３０４に格納されているメディアＩＤ３４１を取り出す（Ｓ６０３）。

【００４５】（３）続いて、乱数を生成し、その乱数と、いま取り出したマスター鍵３２３ａとメディアＩＤ３４１とから、音楽データを暗号化するためのパスワードを生成する（Ｓ６０４）。このときの乱数は、例えば、上記認証において、メモリカード１０９に送信したチャレンジデータ（乱数）を暗号化したもの等を用いる。

（４）得られたパスワードをマスター鍵３２３ａとメディアＩＤ３４１で暗号化し、暗号化キー４２５として認証領域３３２に書き込む（Ｓ６０５）。このときには、データ（暗号化キー４２５）を送信するのに先立ち、認証領域３３２に書き込むためのコマンドを暗号化してメモリカード１０９に送信しておく。

【００４６】（５）最後に、音楽データをパスワードで暗号化しながら暗号化コンテンツ４２６として非認証領域３３１に格納していく（Ｓ６０６）。図９は、音楽データ等のコンテンツをメモリカード１０９から読み出してプレーヤ２０１（及びＰＣ１０２）で再生する動作を示すフロー図である。ここでは、メモリカード１０９内の音楽データをプレーヤ２０１が再生する場合（Ｓ７０１）を説明する。

【００４７】（１）プレーヤ２０１は、デバイス鍵２１１ａ等を用いて、メモリカード１０９の認証部３２１とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモリカード１０９からマスター鍵３２３ａを取り出す（Ｓ７０２）。

（２）次に、専用コマンドを用いて、メモリカード１０９の特殊領域３０４に格納されているメディアＩＤ３４１を取り出す（Ｓ７０３）。

【００４８】（３）続いて、メモリカード１０９の認証領域３３２から音楽データの暗号化キー４２５を取り出す（Ｓ７０４）。このときには、データ（暗号化キー４２５）の読み出しに先立ち、認証領域３３２から読み出すためのコマンドを暗号化してメモリカード１０９に送信しておく。

（４）得られた暗号化キー４２５をマスター鍵３２３ａとメディアＩＤ３４１で復号化し、パスワードを抽出する（Ｓ７０５）。このときの復号化は、図８に示されたステップＳ６０５での暗号化の逆変換である。

【００４９】（５）最後に、非認証領域３３１から暗号化コンテンツ４２６を読み出し、上記ステップＳ７０５で抽出したパスワードで復号しながら音楽を再生していく（Ｓ７０６）。このように、メモリカード１０９の非認証領域３３１に格納された音楽データは、認証領域３３２の暗号化キー４２５がないと復号することができな

い。従って、たとえ不正に音楽データだけを別のメモリカードにコピーしたとしても、その音楽データを正常に再生することができないので、その音楽データの著作権は安全に保護される。

【００５０】また、認証に成功した機器だけがメモリカードの認証領域へのアクセスが許可されるので、認証に用いられるデバイス鍵や暗号化アルゴリズム等を適切に選択して用いることで、一定の条件を満たした機器だけに対してメモリカードの認証領域へのアクセスを許可する等の著作権保護が可能となる。なお、この例では、メモリカード１０９に暗号化コンテンツを記録する際に、その暗号化に用いられたパスワードをマスター鍵とメディアＩＤで暗号化し、暗号化キーとして認証領域３３２に格納されたが（Ｓ６０５）、マスター鍵及びメディアＩＤのいずれかを用いて暗号化することとしてもよい。これによって、暗号の強度が低下する恐れがあるものの、暗号化の簡略化に伴い、メモリカード１０９やプレーヤ２０１等の回路規模が小さくなるという利点が得られる。

【００５１】また、プレーヤ２０１やＰＣ１０２は、認証により、メモリカード１０９からマスター鍵３２３ａを取り出したが、予めプレーヤ２０１やＰＣ１０２にそのマスター鍵３２３ａを埋め込んでおいてもよいし、マスター鍵３２３ａを暗号化し、暗号化マスター鍵として特殊領域３０４に格納しておいてもよい。次に、このようなメモリカードの認証領域の活用例として、「読み出し回数」を格納した例と、「デジタル出力許可回数」を格納した例を示す。

【００５２】図１０は、プレーヤ２０１（及びＰＣ１０２）がメモリカード１０９の認証領域に格納された読み出し回数８１２を操作する動作を示すフロー図である。ここでは、メモリカード１０９に格納された読み出し回数８１２の範囲内でのみ、プレーヤ２０１が、メモリカード１０９の非認証領域３３１に格納された音楽データを音声信号に再生することが許可されている場合（Ｓ８０１）について説明する。

【００５３】（１）プレーヤ２０１は、デバイス鍵２１１ａ等を用いて、メモリカード１０９の認証部３２１とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモリカード１０９からマスター鍵３２３ａを取り出す（Ｓ８０２）。

（２）次に、専用コマンドを用いて、メモリカード１０９の特殊領域３０４に格納されているメディアＩＤ３４１を取り出す（Ｓ８０３）。

【００５４】（３）続いて、メモリカード１０９の認証領域３３２から音楽データの暗号化キー４２５を取り出す（Ｓ７０４）。このときには、データ（暗号化キー４２５）の読み出しに先立ち、認証領域３３２から読み出すためのコマンドを暗号化してメモリカード１０９に送信しておく。

（４）次に、メモリカード１０９の認証領域３３２から読み出し回数８１２を取り出し、その値を検査する（Ｓ８０４）。その結果、その値が無制限な読み出しを許可する旨の値である場合は、図９に示された手順（Ｓ７０４～Ｓ７０６）と同様の手順に従って、音楽を再生する（Ｓ８０６～Ｓ８０８）。

【００５５】（５）一方、読み出し回数８１２が０を示す場合は、もはや再生が許可されていないと判定し（Ｓ８０５）、再生処理を終了する（Ｓ８０９）。そうでない場合は、その読み出し回数８１２を１つ減算し、その結果を認証領域３３２に書き戻した後に（Ｓ８０５）、上記手順に従って、音楽を再生する（Ｓ８０６～Ｓ８０８）。

【００５６】このように、メモリカード１０９の認証領域３３２に、予め許可された再生回数を指定した読み出し回数８１２を格納しておくことにより、プレーヤ２０１による音楽再生の回数をコントロールすることが可能となる。これによって、例えば、レンタルＣＤやＫＩＯＳＫ端末等によるアナログ再生に適用することが可能となる。

【００５７】なお、読み出し回数８１２に代えて、「読み出し時間」とすることで、音楽コンテンツを再生することが可能な総時間を制限することもできる。また、回数と時間とを組み合わせてもよい。さらに、読み出し回数８１２は、再生を開始してから１０秒等の一定時間を超えて再生され続けた場合にだけ、その回数を減算してもよい。また、読み出し回数８１２は、不正な改ざんを防ぐために暗号化して格納することとしてもよい。

【００５８】図１１は、プレーヤ２０１（及びＰＣ１０２）がメモリカード１０９の認証領域に格納されたデジタル出力許可回数９１３を操作する動作を示すフロー図である。ここでは、メモリカード１０９に格納されたデジタル出力許可回数９１３の範囲内でのみ、プレーヤ２０１が、メモリカード１０９の非認証領域３３１に格納された音楽データを読み出してデジタル出力することが許可されている場合（Ｓ９０１）について説明する。

【００５９】（１）プレーヤ２０１は、図９に示された再生の場合（Ｓ７０１～Ｓ７０５）と同様にして、メモリカード１０９と認証を行なった後にマスター鍵３２３ａを取り出し（Ｓ９０２）、メディアＩＤ３４１を取り出し（Ｓ９０３）、暗号化キー４２５を取り出す（Ｓ９０４）、パスワードを抽出する（Ｓ９０５）。

（２）次に、メモリカード１０９の認証領域３３２からデジタル出力許可回数９１３を取り出し、その値を検査する（Ｓ９０６）。その結果、その値が無制限なデジタル出力を許可する旨の値である場合は、非認証領域３３１から暗号化コンテンツ４２６を読み出し、上記ステップＳ９０５で抽出したパスワードで復号しながらデジタルな音楽データとしてデジタル出力端子２０５から出力する（Ｓ９０９）。

【００６０】（３）一方、デジタル出力許可回数９１３が０を示す場合は、もはやデジタル出力は許可されていないと判定し（Ｓ９０８）、アナログ出力による再生だけを行なう（Ｓ９０８）。つまり、非認証領域３３１から暗号化コンテンツ４２６を読み出し、パスワードで復号しながら音楽を再生する（Ｓ９０８）。

（４）読み出したデジタル出力許可回数９１３が０ではない一定の制限回数を示す場合は、その回数を１つ減算し、その結果を認証領域３３２に書き戻した後に（Ｓ９０７）、非認証領域３３１から暗号化コンテンツ４２６を読み出し、上記ステップＳ９０５で抽出したパスワードで復号しながらデジタルな音楽データとしてデジタル出力端子２０５から出力する（Ｓ９０９）。

【００６１】このように、メモリカード１０９の認証領域３３２に、予め許可されたデジタル出力の回数を指定したデジタル出力許可回数９１３を格納しておくことにより、プレーヤ２０１による音楽データのデジタル出力の回数をコントロールすることが可能となる。これによって、例えば、レンタルＣＤやＫＩＯＳＫ端末等によるデジタル再生への適用、即ち、メモリカードに記憶した音楽データのデジタルダビングを著作権者の了解の元に指定した回数分だけコピーを許可するような運用が実現となる。

【００６２】なお、「読み出し回数」の場合と同様に、デジタル出力許可回数９１３に代えて、「デジタル出力許可時間」とすることで、音楽コンテンツをデジタルデータのまま出力することが可能な総時間を制限することもできる。また、回数と時間とを組み合わせてもよい。さらに、デジタル出力許可回数９１３は、その出力を開始してから１０秒等の一定時間を超えて出力され続けた場合にだけ、その回数を減算してもよい。また、デジタル出力許可回数９１３は、不正な改ざんを防ぐために暗号化して格納することとしてもよい。

【００６３】さらに、著作権者に代金を払い込むことで、著作権者が指定した回数だけデジタル出力許可回数を増やす機能を追加してもよい。次に、このメモリカード１０９の物理的なデータ構造（セクタ及びＥＣＣブロックの構造）について説明する。このメモリカード１０９では、フラッシュメモリ３０３に格納されたデータのバックアップと復元に伴う不正行為やデータの改ざんに伴う不正行為等を防止するのに好適なデータ構造が採用されている。つまり、上述のような「読み出し回数」や「デジタル出力許可回数」を認証領域３３２に格納し、それら行為を実行する度にカウントダウンしていく方式では、次のような攻撃を受ける可能性がある。

【００６４】つまり、フラッシュメモリ３０３全体の記憶データを外部の補助記憶装置等にバックアップしておいた後に音楽再生を繰り返し、それら回数が０となった時点でバックアップデータを復元することにより、再び音楽再生を繰り返したり、「読み出し回数」そのものを改ざんすることで、不正に音楽再生を繰り返すことが考えられる。従って、そのような行為を防止する手当てが必要となる。

【００６５】図１２は、メモリカード１０９の認証領域３３２及び非認証領域３３１に共通のデータ構造と、そのデータ構造に対応した読み書き処理のフローとを示す図である。ここでは、コントロールＩＣ３０２の認証部３２１等が有する乱数発生器１００３が発生するカウンター値が時変の鍵として利用される。

【００６６】フラッシュメモリ３０３には、５１２バイトのセクタ１００４ごとに、１６バイトの拡張領域１００５が割り当てられる。各セクタは、カウンター値で暗号化されたデータが格納される。拡張領域１００５は、対応するセクタに格納されている暗号化データの誤り訂正符号を格納するための８バイトのＥＣＣデータ１００６と、その暗号化データの生成に用いられたカウンター値を格納するための８バイトの時変領域１００７とからなる。

【００６７】なお、論理的に（ユーザに開放されたコマンド等を用いて）アクセス可能な領域はセクタ１００４だけであり、拡張領域１００５は、物理的に（メモリカードを読み書きする装置による制御として）のみアクセス可能な領域である。このようなデータ構造とすることで、コマンド等を用いてセクタデータだけが改ざんされても、時変領域１００７の内容は変更されることがないので、それらの整合性を利用することで、不正な改ざんを防止することができる。

【００６８】具体的には、ＰＣ１０２やプレーヤ２０１は、セクタ１００４ごとに、以下の手順に従って、フラッシュメモリ３０３の認証領域３３２や非認証領域３３１にデータを格納したり、読み出したりする。ここでは、まず、ＰＣ１０２がメモリカード１０９にデータを書き込む場合（Ｓ１００１）の手順を説明する。

（１）ＰＣ１０２は、メモリカード１０９に対してカウンター値の発行を要求する。すると、メモリカード１０９内のコントロールＩＣ３０２は、内部の乱数発生器１００３で乱数を発生し（Ｓ１００５）、その乱数をカウンター値としてＰＣ１０２等に送る（Ｓ１００２）。

【００６９】（２）取得したカウンター値と、既に取得しているマスター鍵３２３ａ及びメディアＩＤ３４１とからパスワードを生成する（Ｓ１００３）。

（３）書き込むべき１セクタ分のデータをパスワードで暗号化しながら、メモリカード１０９に送る（Ｓ１００４）。このとき、書き込むべきセクタを指定する情報や、暗号化に用いたカウンター値も一緒に送る

（４）メモリカード１０９は、受け取った暗号化データを、指定されたセクタ１００４に書き込む（Ｓ１００６）。

【００７０】（５）その暗号化データからＥＣＣを計算し、上記セクタに対応する拡張領域１００５に、ＥＣＣ

データ１００６として書き込む（Ｓ１００７）。
（６）続いて、上記暗号化データとともに受け取ったカウンター値を時変領域１００７に書き込む（Ｓ１００８）。
次に、ＰＣ１０２がメモリカード１０９からデータを読み出す場合（Ｓ１０１１）の手順を説明する。
【００７１】（１）ＰＣ１０２は、メモリカード１０９に対して、セクタを指定するとともにデータの読み出しを要求する。すると、メモリカード１０９は、まず、指定されたセクタ１００４の暗号化データだけを読み出してＰＣ１０２に出力し（Ｓ１０１６）、ＰＣ１０２は、その暗号化データを受け取る（Ｓ１０１２）。
（２）次に、メモリカード１０９は、指定されたセクタ１００４に対応する拡張領域１００５の時変領域１００７に格納されたカウンター値を読み出してＰＣ１０２に出力し（Ｓ１０１７）、ＰＣ１０２は、そのカウンター値を受け取る（Ｓ１０１３）。
【００７２】（３）読み出したカウンター値と、既に取得しているマスター鍵３２３ａ及びメディアＩＤ３４１とからパスワードを生成する（Ｓ１０１４）。
（４）そのパスワードを用いて、暗号化データを復号する（Ｓ１０１５）。
ここで、もし、不正な改ざん等により、セクタ１００４のデータが変更されている場合には、時変領域１００７から読み出されたカウンター値との不整合が生じ、元のデータに復元されない。
【００７３】このように、フラッシュメモリ３０３内に、ユーザからは見えない（アクセスできない）隠し領域としての時変領域１００７を設け、そこに格納されたカウンター値に依存したパスワードでデータを暗号化し格納することで、不正なユーザによるデータの改ざんを防止することができる。なお、ここでは、時変領域１００７は、ＥＣＣを格納するための拡張領域１００５としたが、メモリカードの外部から書き換えができない領域であれば、フラッシュメモリ３０３内の他の領域に設けてもよい。
【００７４】また、カウンター値は、乱数であったが、刻々と変化する時刻等のタイマー値としたり、フラッシュメモリ３０３への書き込み回数を示す値としてもよい。次に、フラッシュメモリ３０３の論理アドレスと物理アドレスとの対応づけについて、好ましい例を説明する。図１３は、論理アドレスと物理アドレスとの対応を変更する様子を示す図であり、（ａ）は変更前の対応関係、（ｂ）は変更後の対応関係、（ｃ）は（ａ）に対応する変換テーブル１１０１、（ｄ）は（ｂ）に対応する変換テーブル１１０１を示す。
【００７５】ここで、変換テーブル１１０１は、全ての論理アドレス（ここでは、論理ブロックの番号）と各論理アドレスに対応する物理アドレス（ここでは、フラッシュメモリ３０３を構成する物理ブロックの番号）とを組にして記憶するテーブルであり、コントロールＩＣ３０２内の不揮発な記憶領域等に保存され、認証領域アクセス制御部３２５や非認証領域アクセス制御部３２６によって論理アドレスを物理アドレスに変換する際等において参照される。
【００７６】メモリカード１０９にアクセスする機器は、メモリカード１０９中の物理的に存在するすべてのデータ空間（フラッシュメモリ３０３を構成する全ての物理ブロック）にデータを書き込めるのではなく、論理アドレスによって特定できる論理的なデータ空間（論理ブロック）にのみデータを書き込むことができる。この理由の一つは、フラッシュメモリ３０３の一部が破損し読み書きが行えなくなった場合に、その領域を置き換えるための代替領域を確保しておかなければならないからである。そして、そのような欠陥ブロックを代替領域中のブロックと置き換えた場合であっても、その対応づけの変更を変換テーブルに反映しておくことで、複数の連続する物理ブロックからなるファイルの論理的な連続性は維持されるので、外部機器に対しては破損が生じなかったように見せかけることができる。
【００７７】ところが、複数のブロックからなるファイル等をメモリカード１０９に格納したり、削除したりすることを繰り返していると、論理ブロックのフラグメンテーションが増大する。つまり、図１３（ａ）に示されるように、同一のファイルfile1を構成する論理ブロックであるにも拘わらず、それらの論理アドレスが不連続となってしまう。
【００７８】これでは、例えば、音楽データをメモリカード１０９に格納しようとしたときに、メモリカード１０９の論理的な連続領域に書けないので、各ブロック毎に書き込みコマンド「Write address count」を発行する必要があり、書き込み速度が低下してしまう。同様に、読み出し動作においても、１曲を構成する音楽データであるにも拘わらず、各ブロック毎に読み出しコマンド「Read address count」を発行する必要があり、音楽データのリアルタイム再生が困難となってしまう。
【００７９】この問題を解決する方法として、このメモリカード１０９のコントロールＩＣ３０２は、外部機器からのコマンドに基づいて、変換テーブル１１０１を書き換える機能を有する。具体的には、コントロールＩＣ３０２のコマンド判定制御部３２２は、変換テーブル１１０１を書き換えるための専用コマンドがコマンドピンから入力されると、そのコマンドを解釈し、続いて送られてくるパラメータを用いて変換テーブル１１０１を書き換える。
【００８０】その具体的な動作は、図１３に示される通りである。いま、上記専用コマンドが送られてくる前においては、フラッシュメモリ３０３において、図１３（ａ）に示されるように、物理アドレス０及び２にファイルfile1を構成するデータが存在し、物理アドレス１

にファイルfile2を構成するデータが存在するとする。そして、変換テーブル１１０１には、図１３（ｃ）に示されるように、物理アドレスと論理アドレスとが一致する内容が保持されているとする。つまり、物理アドレス上と同様に、論理アドレス上においても、ファイルfile2のデータが別のファイルfile1のデータに挟まれて格納されているとする。

【００８１】このような状態を解消しようとうする外部機器は、フラッシュメモリ３０３に対して、特定のファイルfile1の連続性を確保する旨を示す上記専用コマンド及びパラメータを送る。すると、メモリカード１０９のコマンド判定制御部３２２は、その専用コマンド及びパラメータに従って、変換テーブル１１０１を図１３（ｄ）に示される内容に書き換える。つまり、フラッシュメモリ３０３の論理及び物理アドレスの対応関係は、図１３（ｂ）に示されるように変更される。

【００８２】図１３（ｂ）に示された関係図から分かるように、物理ブロックの配置は変化していないにも拘わらず、ファイルfile1を構成する２つの論理ブロックが連続するように再配置されている。これによって、その外部機器は、次回のアクセス以降においては、それまでよりも高速にファイルfile1にアクセスすることが可能となる。

【００８３】以上のような変換テーブル１１０１の変更は、論理ブロックのフラグメンテーションを解消するためだけでなく、フラッシュメモリ３０３の認証領域３３２と非認証領域３３１それぞれのサイズを変更する場合にも用いられる。このときには、サイズを小さくする領域の物理ブロックがサイズを大きくする領域の物理ブロックとして割り当てられるように変換テーブル１１０１を書き換えるだけで済むので、高速な領域変更が可能となる。

【００８４】次に、このメモリカード１０９が有する未消去ブロックに関する機能、具体的には、未消去リストコマンド及び消去コマンドを受信した場合の動作について説明する。ここで、未消去ブロックとは、フラッシュメモリ３０３内の物理ブロックであって、過去に書き込みが行なわれ、かつ、物理的に未消去状態となっているブロックをいう。つまり、未消去ブロックは、次に使用される（書き込まれる）前に一括消去が必要とされる物理ブロックである。

【００８５】また、未消去リストコマンドとは、コマンド判定制御部３２２が解釈及び実行可能なコマンドのひとつであり、その時点におけるフラッシュメモリ３０３に存在する全ての未消去ブロックの番号の一覧を取得するためのコマンドである。メモリカード１０９に使用されているフラッシュメモリ３０３は、書き込みを行う前にブロック単位での一括消去が必要とされるが、その消去処理は書き込み時間の半分近くを占めるため、予め消去しておいた方がより高速に書き込むことができる。そこで、このメモリカード１０９は、その便宜を図るために、未消去リストコマンドと消去コマンドを外部機器に提供している。

【００８６】いま、フラッシュメモリ３０３は、図１４（ａ）に示されるような論理ブロック及び物理ブロックの使用状態とする。ここでは、論理ブロック０～２が使用中であり、物理ブロック０～２、４及び５が未消去ブロックとなっている。この状態においては、コマンド判定制御部３２２内に保持されている未消去リスト１２０３は、図１４（ｂ）に示される内容となっている。ここで、未消去リスト１２０３は、フラッシュメモリ３０３を構成する全ての物理ブロックに対応するエントリーからなる記憶テーブルであり、コマンド判定制御部３２２による制御の下で、対応する物理ブロックの消去状態に応じた値（消去済みの場合は“０”、未消去の場合は“１”）が保持される。

【００８７】図１４（ｃ）は、このような状態においてＰＣ１０２やプレーヤ２０１が未消去リストコマンドと消去コマンドを用いて事前にブロックを消去する場合の動作を示すフロー図である。なお、フラッシュメモリ３０３には、図１４（ｄ）に示されるように、論理ブロックの使用状態を示すＦＡＴ（File Allocation Table）等のテーブルが格納されているものとする。

【００８８】ＰＣ１０２やプレーヤ２０１等の外部機器は、例えば、メモリカード１０９へのアクセスが発生していないアイドル時間において、このメモリカード１０９に対して未消去リストコマンドを発行する（Ｓ１２０１）。そのコマンドを受け取ったメモリカード１０９のコマンド判定制御部３２２は、内部に有する未消去リスト１２０３を参照することで、状態値１が登録されている物理ブロックの番号０～２、４及び５を特定し、その外部機器に返す。

【００８９】続いて、外部機器は、フラッシュメモリ３０３に格納された図１４（ｄ）に示される論理ブロックの使用状態を示すテーブルを参照することで、論理的に使用されていないブロックを特定する（ステップＳ１２０２）。そして、上記２つのステップＳ１２０１及びＳ１２０２で取得した情報に基づいて、消去可能なブロック、即ち、論理的に不使用で、かつ、物理的に未消去なブロック（ここでは、物理ブロック４と５）を特定した後に（ステップＳ１２０３）、メモリカード１０９に対して、それらブロック４と５の番号を指定した消去コマンドを発行する（ステップＳ１２０４）。そのコマンドを受信したメモリカード１０９のコマンド判定制御部３２２は、アクセス制御部３２５、３２６に指示を出す等により、指定された物理ブロック４と５を一括消去する。

【００９０】これによって、もし、その物理ブロック４と５への書き込みが発生した場合には、その物理ブロックに対する消去処理は不要となるので、高速な書き込み

が可能となる。次に、このメモリカード１０９が有する個人データの保護に関する機能、具体的には、メモリカード１０９が外部機器を認証する際にその外部機器を使用するユーザの個人データを必要とする場合における個人データの保護機能について説明する。ここで、個人データとは、そのユーザを一意に識別するためのデータであって、メモリカード１０９の認証領域３３２へのアクセスが許可された正規のユーザとしてメモリカード１０９に識別させるためのデータである。

【００９１】このような場合において、認証領域３３２へのアクセスの度にユーザに対して繰り返し個人データを入力することを要求したり、その個人データを認証領域３３２に格納することとしたのでは、不正者によって盗聴されたり、認証領域３３２にアクセスする権限を有する他のユーザによって見られたりする不都合がある。

【００９２】これを防止するために、音楽データと同様に、個人データについても、個人が設定したパスワードで暗号化してから格納するという方法が考えられる。しかしながら、パスワードを設定した場合には、その個人データを見るたびにパスワードを入力しなければならず、手続が面倒であり、その管理も必要となる。そこで、このメモリカード１０９は、不必要に個人データを繰り返し入力することを回避する機能を有する。

【００９３】図１５は、認証のためのプレーヤ２０１とメモリカード１０９間の通信シーケンス及び主要な構成要素を示す図である。なお、本図に示される処理は、主にプレーヤ２０１の認証回路２１６及びメモリカード１０９の認証部３２１によって実現される。本図に示されるように、プレーヤ２０１の認証回路２１６は、暗号化及び復号化等の機能の他に、メモリカード１０９に保持されたマスター鍵３２３ａと同一の秘密鍵であるマスター鍵１３０１と、製造番号（ｓ／ｎ）等のプレーヤ２０１に固有のＩＤである機器固有ＩＤ１３０２とを予め記憶している。

【００９４】また、メモリカード１０９の認証部３２１は、暗号化、復号化及び比較等の機能に他に、２つの不揮発な記憶領域である機器固有ＩＤ群記憶領域１３１０とユーザキー記憶領域１３１１とを有する。機器固有ＩＤ群記憶領域１３１０は、このメモリカード１０９の認証領域３３２へのアクセスが許可された全ての機器の機器固有ＩＤを記憶しておくための記憶領域であり、ユーザキー記憶領域１３１１は、個人データとして機器から送られてきたユーザキーを記憶しておくための記憶領域である。

【００９５】具体的な認証手順は、以下の通りである。なお、送受信においては、全てのデータは暗号化されて送信され、受信側で復号される。そして、手順が進む度に、次の手順での暗号化及び復号化に用いられる鍵が生成される。

（１）メモリカード１０９とプレーヤ２０１とを接続すると、まず、プレーヤ２０１は、マスター鍵１３０１を用いて機器固有ＩＤ１３０２を暗号化し、メモリカード１０９に送る。

【００９６】（２）メモリカード１０９は、受け取った暗号化された機器固有ＩＤ１３０２をマスター鍵３２３ａで復号し、得られた機器固有ＩＤ１３０２が既に機器固有ＩＤ群記憶領域１３１０に格納されているか検査する。

（３）その結果、既に機器固有ＩＤ１３０２が格納されている場合は、認証が成功した旨をプレーヤ２０１に通知し、一方、機器固有ＩＤ１３０２が格納されていない場合は、プレーヤ２０１に対しユーザキーを要求する。

【００９７】（４）プレーヤ２０１は、ユーザキーの入力をユーザに促した後に、ユーザから個人データとしてのユーザキーを取得し、そのユーザキーをメモリカード１０９に送る。

（５）メモリカード１０９は、送られてきたユーザキーと予めユーザキー記憶領域１３１１に格納されているものとを比較し、一致している場合、又は、ユーザキー記憶領域１３１１が空であった場合は、認証が成功した旨をプレーヤ２０１に通知するとともに、上記ステップ（３）で獲得した機器固有ＩＤ１３０２を機器固有ＩＤ群記憶領域１３１０へ格納する。

【００９８】これによって、ユーザが所有する機器とメモリカード１０９とを初めて接続した場合は個人データ（ユーザキー）の入力が必要とされるが、２回目以降においては、その機器の機器固有ＩＤが用いられて自動的に認証が成功するので、再び、個人データの入力を要求されることはない。次に、本メモリカード１０９とＰＣ１０２やプレーヤ２０１等の外部機器との認証プロトコルの変形例について、図１６及び図１７を用いて説明する。

【００９９】図１６は、変形例に係るメモリカード１０９と外部機器（ここでは、プレーヤ２０１）との認証手順を示す通信シーケンス図である。ここでの処理は、主に、変形例に係るプレーヤ２０１の認証回路２１６、ＰＣ１０２の制御プログラム１１１ｂ及びメモリカード１０９の認証部３２１によって実現される。また、メモリカード１０９のマスター鍵記憶部３２３には、暗号化されたマスター鍵（暗号化マスター鍵３２３ｂ）が格納されており、特殊領域３０４には、メディアＩＤ３４１に加えて、そのメディアＩＤ３４１を暗号化して得られるセキュアメディアＩＤ３４３も格納されているものとする。

【０１００】まず、プレーヤ２０１は、メモリカード１０９にコマンドを発することで、メモリカード１０９のマスター鍵３２３ｂを取り出し、デバイス鍵２１１ａで復号する。ここでの復号アルゴリズムは、メモリカード１０９に格納されている暗号化マスター鍵３２３ｂが生成された際に用いられた暗号アルゴリズムに対応する。

従って、このプレーヤ２０１が有するデバイス鍵２１１ａが予定されたもの（正規のもの）であれば、この復号によって元のマスター鍵に復元される。

【０１０１】続いて、プレーヤ２０１は、メモリカード１０９にコマンドを発することで、メモリカード１０９のメディアＩＤ３４１を取り出し、復元された上記マスター鍵で暗号化する。ここでの暗号アルゴリズムは、メモリカード１０９に格納されているセキュアメディアＩＤ３４３が生成された際に用いられた暗号アルゴリズムと同一である。従って、ここでの暗号化によって、メモリカード１０９が有するセキュアメディアＩＤ３４３と同一のセキュアメディアＩＤが得られる。

【０１０２】続いて、それらセキュアメディアＩＤそれぞれを用いて、プレーヤ２０１とメモリカード１０９は、相互認証を行なう。その結果、いずれの機器においても、相手機器の認証に成功したか否かを示す（ＯＫ／ＮＧ）情報と、その認証結果に依存して定まる時変の鍵であるセキュア鍵とが生成される。このセキュア鍵は、双方の機器２０１及び１０９が認証に成功した場合にのみ一致し、かつ、相互認証を繰り返す度に変動する性質を有する。

【０１０３】続いて、相互認証に成功すると、プレーヤ２０１は、メモリカード１０９の認証領域３３２にアクセスするためのコマンドを生成する。具体的には、例えば、認証領域３３２からデータを読み出す場合であれば、そのコマンド「SecureReadaddress　count」のパラメータ（２４ビット長のアドレス「address」と８ビット長のカウント「count」）をセキュア鍵で暗号化し、得られた暗号化パラメータと、そのコマンドのタグ（コマンドの種類「SecureRead」を示す６ビット長のコード）とを連結して得られる暗号化コマンドをメモリカード１０９に送る。

【０１０４】暗号化コマンドを受け取ったメモリカード１０９は、そのタグからコマンドの種類を判定する。ここでは、認証領域３３２からの読み出しコマンド「SecureRead」であると判定する。その結果、認証領域３３２へのアクセスコマンドであると判定した場合には、そのコマンドに含まれていたパラメータを、相互認証で得られたセキュア鍵で復号する。ここでの、復号アルゴリズムは、プレーヤ２０１において暗号化コマンドを生成する際に用いられた暗号アルゴリズムに対応するので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復号によって得られるパラメータは、プレーヤ２０１で用いられた元のパラメータに等しくなる。

【０１０５】そして、メモリカード１０９は、復号されたパラメータによって特定されるセクタに格納された暗号化キー４２５を認証領域３３２から読み出し、それをセキュア鍵により暗号化しプレーヤ２０１に送信する。プレーヤ２０１は、送られてきたデータを、相互認証で得られたセキュア鍵を用いて復号する。ここでの、復号アルゴリズムは、メモリカード１０９において暗号化キー４２５の暗号化に用いられたアルゴリズムに対応するので、相互認証が成功していれば、即ち、双方の機器で用いられるセキュア鍵が一致していれば、この復号によって得られるデータは、元の暗号化キー４２５に一致する。

【０１０６】なお、メモリカード１０９は、認証領域３３２へのアクセスコマンドの実行を終える度に、それに用いたセキュア鍵を破棄（消去）する。これによって、メモリカード１０９の認証領域３３２にアクセスする外部機器は、１個のコマンドを送出する度に、事前に相互認証を行い、それにパスしている必要がある。図１７は、図１６に示された相互認証における詳細な手順を示す通信シーケンス図である。ここでは、メモリカード１０９とプレーヤ２０１は、チャレンジ・レスポンス型の相互認証を行う。

【０１０７】メモリカード１０９は、プレーヤ２０１の正当性を検証するために、乱数を生成し、それをチャレンジデータとしてプレーヤ２０１に送る。プレーヤ２０１は、自己の正当性を証明するために、そのチャレンジデータを暗号化し、レスポンスデータとしてメモリカード１０９に返す。メモリカード１０９は、そのレスポンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、プレーヤ２０１の認証に成功した（ＯＫ）と認識し、そのプレーヤ２０１から送られてくる認証領域３３２へのアクセスコマンドを受け付ける。一方、比較の結果、一致しなかった場合には、認証に成功しなかった（ＮＧ）したと認識し、もし、その後にプレーヤ２０１から認証領域３３２へのアクセスコマンドが送られてきたとしても、その実行を拒絶する。

【０１０８】同様にして、プレーヤ２０１は、メモリカード１０９の正当性を検証するために、上記認証と同様のやりとりを行う。つまり、乱数を生成し、それをチャレンジデータとしてメモリカード１０９に送る。メモリカード１０９は、自己の正当性を証明するために、そのチャレンジデータを暗号化し、レスポンスデータとしてプレーヤ２０１に返す。プレーヤ２０１は、そのレスポンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、メモリカード１０９の認証に成功した（ＯＫ）と認識し、そのメモリカード１０９の認証領域３３２へのアクセスコを行う。一方、比較の結果、一致しなかった場合には、認証に成功しなかった（ＮＧ）したと認識し、そのメモリカード１０９の認証領域３３２へのアクセスは断念する。

【０１０９】なお、これら相互認証における暗号化アルゴリズムは、メモリカード１０９及びプレーヤ２０１が正当な機器である限り、全て同一である。また、メモリ

カード１０９及びプレーヤ２０１は、それぞれの認証及び証明において生成した暗号化チャレンジデータとレスポンスデータとを排他的論理和演算し、得られた結果をセキュア鍵として、メモリカード１０９の認証領域３３２へのアクセスのために用いる。そうすることで、双方の機器１０９及び２０１が相互認証に成功した場合にのみ共通となり、かつ、時変のセキュア鍵を共有し合うことが可能となり、これによって、認証領域３３２にアクセスする条件として相互認証に成功していることが条件とされることになる。

【０１１０】なお、セキュア鍵の生成方法として、暗号化チャレンジデータとレスポンスデータとセキュアメディアＩＤとの排他的論理和をとることとしてもよい。次に、本メモリカード１０９の認証領域３３２と非認証領域３３１との境界線の変更機能についての変形例について、図１８及び図１９を用いて説明する。図１８は、境界線を変更する前のフラッシュメモリ３０３の使用状態を示す図である。図１８（ａ）は、フラッシュメモリ３０３の物理ブロックの構成を示すメモリマップである。

【０１１１】図１８（ｂ）は、非認証領域アクセス制御部３２６内の不揮発な記憶領域等に置かれる非認証領域３３１専用の変換テーブル１１０３であり、非認証領域３３１の論理ブロックと物理ブロックとの対応関係が格納されている。非認証領域アクセス制御部３２６は、この変換テーブル１１０３を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【０１１２】図１８（ｃ）は、認証領域アクセス制御部３２５内の不揮発な記憶領域等に置かれる認証領域３３２専用の変換テーブル１１０２であり、認証領域３３２の論理ブロックと物理ブロックとの対応関係が格納されている。認証領域アクセス制御部３２５は、この変換テーブル１１０２を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【０１１３】境界線の変更前においては、図１８（ａ）に示されるように、フラッシュメモリ３０３の代替領域を除いた記憶領域（物理ブロック０００〜ＥＦＦＦ）のうち、境界線よりも下位アドレスに位置する物理ブロック００００〜ＤＦＦＦが非認証領域３３１に割り当てられ、上位アドレスに位置する物理ブロックＥ０００〜ＥＦＦＦが認証領域３３２に割り当てられている。

【０１１４】そして、図１８（ｂ）に示された変換テーブル１１０２から分かるように、非認証領域３３１においては、物理ブロックと論理ブロックの番号が一致するように対応づけられている。一方、図１８（ｃ）に示された変換テーブル１１０３から分かるように、認証領域３３２においては、物理ブロックと論理ブロックとは、その番号の並びが逆順になっている。つまり、論理ブロック００００〜０ＦＦＦそれぞれが物理ブロックＥＦＦＦ〜Ｅ０００に対応している。これは、論理ブロックは昇順に使用されていくことと、境界線が移動された場合において領域変更の生じた物理ブロックのデータ退避や移動処理の手間を考慮したからである。

【０１１５】図１９（ａ）〜（ｃ）は、境界線を変更した後のフラッシュメモリ３０３の使用状態を示す図であり、それぞれ、変更前の図１８（ａ）〜（ｃ）に対応する。なお、境界線の変更は、そのアドレスを指定する専用のコマンドがコマンドピンからコマンド判定制御部３２２に入力されたときに、コマンド判定制御部３２２によって認証領域アクセス制御部３２５内の変換テーブル１１０２及び非認証領域３３１内の変換テーブル１１０３が書き換えられることにより、実現される。

【０１１６】図１９（ａ）〜（ｃ）に示されるように、ここでは、物理ブロックＥ０００とＤＦＦＦ間に置かれていた境界線が物理ブロックＤ０００とＣＦＦＦ間に移動されている。つまり、非認証領域３３１のサイズを１０００（hex）個だけ減少させ、認証領域３３２のサイズを１０００（hex）だけ増加させている。それに伴って、図１９（ｂ）に示されるように、非認証領域３３１の変換テーブル１１０３のサイズは、１０００（hex）個のエントリー分だけ減少され、その結果、論理ブロック０００〜ＣＦＦＦに対応する物理ブロック０００〜ＣＦＦＦが示されている。一方、図１９（ｃ）に示されるように、認証領域３３２の変換テーブル１１０２のサイズは、１０００（hex）個のエントリー分だけ増加され、その結果、論理ブロック０００〜１ＦＦＦに対応する物理ブロックＥＦＦＦ〜Ｄ０００が示されている。

【０１１７】このように、フラッシュメモリ３０３の一定領域において境界線によって非認証領域と認証領域とを区切り、その境界線の移動によって各領域のサイズを変更することにより、このメモリカード１０９の多様な応用、例えば、保護すべきデジタル著作物の格納を主要な用途とする場合やその逆の場合等に対応させることが可能となる。

【０１１８】そして、非認証領域及び認証領域いずれにおいても、境界線に遠いアドレスの物理ブロックから境界線に近いアドレスの物理ブロックに向かって、使用していくように論理ブロックと物理ブロックとを対応づけることで、境界線の移動に伴うデータ退避や移動処理等の手間が削減される。また、そのような対応づけは、認証領域３３２専用の変換テーブル１１０２と非認証領域３３１専用の変換テーブル１１０３とに分離して設けることで、その実現が容易となる。

【０１１９】なお、認証領域３３２においては、ブロックの単位で論理アドレスと物理アドレスとが逆順になっていたが、このような単位に限られず、例えば、セクタの単位で逆順としたり、バイトの単位で逆順としてもよい。以上、本発明のメモリカードについて、実施の形態

及び変形例を用いて説明したが、本発明はこれらに限定されるものではない。

【０１２０】例えば、ＰＣ１０２やプレーヤ２０１は、メモリカード１０９の認証領域３３２にアクセスするためのコマンドを発する度に同じ手順によるメモリカード１０９との認証が必要とされたが、コマンドの種類によっては簡略化された認証手順でアクセスできるようにしてもよい。例えば、書き込みコマンド「SecureWrite」については、メモリカード１０９から暗号化マスター鍵３２３ｂやメディアＩＤ３４１を取り出す必要はなく、片方向の認証（メモリカード１０９による機器の認証だけ）に成功するだけで、メモリカード１０９により実行されるとしてもよい。これによって、あまり著作権保護との関連が強くないコマンドについては、その実行速度が高速化される。

【０１２１】また、本発明のメモリカード１０９が有するフラッシュメモリ３０３を他の記憶メディア、例えば、ハードディスク、光ディスク、光磁気ディスク等の不揮発メディアに置き換えても本発明と同様の著作権保護が可能な携帯型記憶カードが実現されることは言うまでもない。

【０１２２】

【発明の効果】以上の説明から明らかなように、本発明に係る半導体メモリカードは、電子機器に着脱可能な半導体メモリカードであって、書き換え可能な不揮発メモリと、前記不揮発メモリ内の予め定められた２つの記憶領域である認証領域と非認証領域への前記電子機器によるアクセスを制御する制御回路と、前記認証領域及び前記非認証領域それぞれの領域サイズを変更する領域サイズ変更回路を備え、前記制御回路は、前記非認証領域への前記電子機器によるアクセスを制御する非認証領域アクセス制御部と、前記電子機器の正当性を検証するために前記電子機器の認証を試みる認証部と、前記認証部が認証に成功した場合にだけ前記認証領域への前記電子機器によるアクセスを許可する認証領域アクセス制御部とを有し、前記認証領域と前記非認証領域は、前記不揮発性メモリ内の一定サイズの連続した記憶領域を２分して得られる各領域に割り当てられ、前記領域サイズ変更回路は、前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、前記電子機器からの命令に従って前記認証領域変換テーブル及び前記認証領域変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を２分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられていることを特徴とする。

【０１２３】これにより、著作権保護に関わるデータを認証領域に格納し、そうでないデータを非認証領域に格納することで、デジタル著作物と非著作物とを混在させて使用することができ、両方の用途を兼ね備えた半導体メモリカードが実現される。前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられているので、論理アドレスの昇順に使用していくことにより、認証領域と非認証領域との境界付近の領域が使用される確率が低くなる。故に、その境界を移動させた場合に必要とされるデータ退避や移動等の処理が発生する確率も低くなり、領域サイズの変更が簡単化される。

【０１２４】前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御するので、同一ファイルを構成する複数の論理ブロックが断片化する現象が生じても、論理的に連続した論理ブロックとなるように容易に変更することができるので、同一ファイルへのアクセスが高速化される。

【０１２５】ここで、前記認証部は、認証の結果を反映した鍵データを生成し、前記認証領域アクセス制御部は、前記電子機器から送られてくる暗号化された命令を前記認証部が生成した鍵データで復号し、復号された命令に従って前記認証領域へのアクセスを制御するとしてもよい。これによって、半導体メモリカードと電子機器とのやりとりが盗聴されたとしても、認証領域にアクセスするための命令は、直前に行われた認証結果に依存して暗号化されているので、認証領域への不正なアクセスに対する防止機能が高くなる。

【０１２６】また、前記認証部は、前記電子機器とチャレンジ・レスポンス型の相互認証を行い、前記電子機器の正当性を検証するために前記電子機器に送信したチャレンジデータと自己の正当性を証明するために生成したレスポンスデータとから前記鍵データを生成するとしてもよい。これによって、鍵データは、半導体メモリカードと電子機器の双方が相互認証に成功したときにのみ初めて双方において共有され、かつ、認証の度に変化するという性質を有するので、そのような鍵データを用いなければアクセスすることができない認証領域の安全性はより強いものとなる。

【０１２７】また、前記電子機器から送られてくる暗号化された命令は、前記認証領域へのアクセスの種別を特定する暗号化されていないタグ部と、アクセスする領域を特定する暗号化されたアドレス部とからなり、前記認証部は、前記鍵データを用いて、前記命令のアドレス部を復号し、復号されたアドレスによって特定される領域に対して、前記命令のタグ部によって特定される種別のアクセスを実行制御するとしてもよい。

【０１２８】これによって、命令のアドレス部だけが暗号化されるので、このような命令を受け取った半導体メモリカードでの復号や解読処理は簡易となる。また、前記半導体メモリカードはさらに、他の半導体メモリカードと区別して自己を特定することが可能な固有の識別データを予め記憶する識別データ記憶回路を備え、前記認証部は、前記識別データ記憶回路に格納された識別データを用いて相互認証を行い、前記識別データに依存させて前記鍵データを生成するとしてもよい。

【０１２９】これによって、相互認証においては、個々の半導体メモリカードに依存したデータが交換されるので、不正な相互認証の解読に対して高い安全性を維持することができる。また、前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備えてもよい。これによって、他の半導体メモリカードと区別できる識別データ等を読み出し専用メモリに格納し、デジタル著作物をその識別データに依存させて格納したりすることで、著作権保護の機能が強化される。

【０１３０】また前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化データに対応づけられた前記読み出し専用の記憶領域に書き込むとしてもよい。

【０１３１】これによって、読み書き可能な記憶領域に対する不正な改ざん等が行われても、読み出し専用の記憶領域に格納された乱数との整合性を検査することで、そのような行為を検出することが可能となるので、より安全なデータ記録が実現される。前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有してもよい。これによって、半導体メモリカードを破壊して認証領域及び非認証領域のメモリ内容を直接読み出す等の不正な攻撃に耐えることが可能となる。

【０１３２】また、前記不揮発メモリは、フラッシュメモリであり、前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有してもよい。これによって、電子機器は、フラッシュメモリの書き換えに先立って、未消去の領域を知り、その領域を事前に消去しておくことができるので、高速な書き換えが可能となる。

【０１３３】また、前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有してもよい。

【０１３４】これによって、半導体メモリカードと接続して使用する度にパスワードや個人データの入力が要求されるという手間が回避されるので、不正に個人データが盗聴されて利用されるという不具合の発生が抑えられる。本発明に係る読み出し装置は、上記半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、前記読み出し装置は、前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているか否か判断する判断手段と、許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする。

【０１３５】これによって、半導体メモリカードに格納されたデジタル著作物の読み出し回数を制限することが可能となり、音楽コンテンツの有料レンタル等への適用が可能となる。また、本発明に係る読み出し装置は、上記半導体メモリカードに格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、前記読み出し装置は、前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているか否か判断

する判断手段と、許可されている場合にのみ前記デジタル著作物をデジタル信号のまま外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする。

【0136】これによって、半導体メモリカードに格納されたデジタル著作物のデジタルコピーの回数を制限することが可能となり、著作権者の意図に沿った木目の細かい著作権保護が可能となる。このように、本発明は、デジタル著作物の記録媒体としての用途とコンピュータの補助記憶装置としての用途の両方を兼ね備えた柔軟な機能を有する半導体メモリカード等であり、特に 電子音楽配信に伴うデジタル著作物の健全な流通を確保するという効果を奏し、その実用的価値は極めて大きい。

【図面の簡単な説明】

【図1】本発明の実施の形態における電子音楽配信に係るパソコンと、そのPCに着脱可能な半導体メモリカードの外観を示す図である。

【図2】同半導体メモリカードを記録媒体とする携帯型のプレーヤの外観を示す図である。

【図3】同パソコンのハードウェア構成を示すブロック図である。

【図4】同プレーヤのハードウェア構成を示すブロック図である。

【図5】同半導体メモリカードの外観及びハードウェア構成を示す図である。

【図6】同パソコンや同プレーヤから見た同半導体メモリカードの記憶領域の種類を示す図である。

【図7】同パソコンや同プレーヤが同半導体メモリカードの各領域にアクセスする際の制限やコマンドの形態を示す図であり、（a）は各領域へのアクセスにおけるルールを示し、（b）は各領域のサイズの変更におけるルールを示し、（c）は同半導体メモリカードの領域を示す概念図である。

【図8】音楽データ等のコンテンツを同パソコン（及び同プレーヤ）が同半導体メモリカードに書き込む動作を示すフロー図である。

【図9】音楽データ等のコンテンツを同半導体メモリカードから読み出して同プレーヤ（及び同パソコン）で再生する動作を示すフロー図である。

【図10】同プレーヤ（及び同パソコン）が同半導体メモリカードの認証領域に格納された読み出し回数を操作する動作を示すフロー図である。

【図11】同プレーヤ（及び同パソコン）が同半導体メモリカードの認証領域に格納されたデジタル出力許可回数を操作する動作を示すフロー図である。

【図12】同半導体メモリカードの認証領域及び非認証領域に共通のデータ構造と、そのデータ構造に対応した読み書き処理のフローとを示す図である。

【図13】同半導体メモリカードの論理アドレスと物理アドレスとの対応を変更する様子を示す図であり、（a）は変更前の対応関係、（b）は変更後の対応関係、（c）は（a）に対応する変換テーブル、（d）は（b）に対応する変換テーブルを示す。

【図14】同半導体メモリカードが有する未消去ブロックに関する機能を説明する図であり、（a）は論理ブロック及び物理ブロックの使用状態を示し、（b）はその状態における未消去リストを示し、（c）はPC102やプレーヤ201が未消去リストコマンドと消去コマンドを用いて事前にブロックを消去する場合の動作を示すフロー図であり、（d）は論理ブロックの使用状態を示すテーブルである。

【図15】認証のための同プレーヤと同半導体メモリカード間の通信シーケンス及び主要な構成要素を示す図である。

【図16】本発明の変形例に係る同半導体メモリカードと外部機器との認証手順を示す通信シーケンス図である。

【図17】図16に示された相互認証の詳細な手順を示す通信シーケンス図である。

【図18】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更前の状態を示す図であり、（a）はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、（b）は非認証領域専用の変換テーブルを示し、（c）は認証領域専用の変換テーブルを示す。

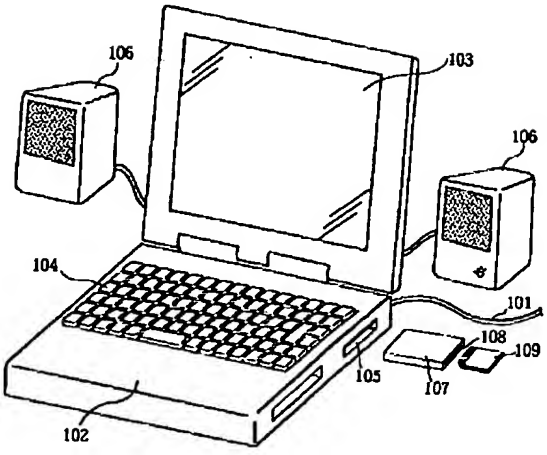
【図19】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更後の状態を示す図であり、（a）はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、（b）は非認証領域専用の変換テーブルを示し、（c）は認証領域専用の変換テーブルを示す。

【符号の説明】

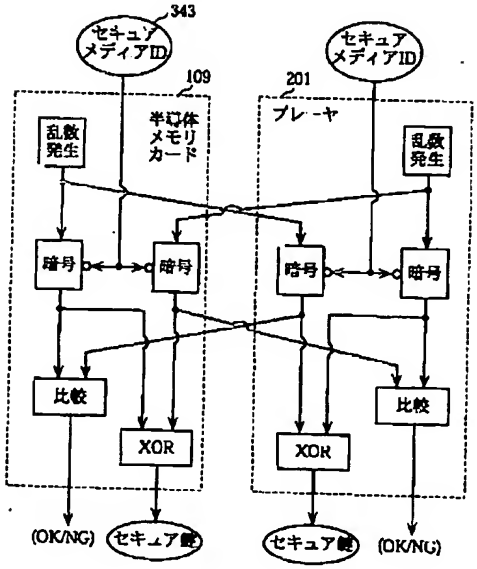
101　通信回線
102　PC
103　ディスプレイ
104　キーボード
105　メモリカードライタ挿入口
106　スピーカ
107　メモリカードライタ
108　メモリカード挿入口
109　メモリカード
110　CPU
111　ROM
112　RAM
113　通信ポート
114　内部バス
117　デスクランブラ
118　AACデコーダ
119　D／Aコンバータ
120　ハードディスク

201　プレーヤ
202　操作ボタン
203　液晶表示部
204　アナログ出力端子
205　デジタル出力端子
206　メモリカード挿入口
208　ヘッドフォン
210　CPU
211　ROM
212　RAM
213　通信ポート
214　内部バス
215　カードI／F部
216　認証回路
217　デスクランブラ
218　AACデコーダ
219　D／Aコンバータ
220　AACエンコーダ
221　A／Dコンバータ
222　スクランブラ
223　アナログ入力端子
224　スピーカ
302　コントロールIC
303　フラッシュメモリ
304　ROM（特殊領域）
321　認証部
322　コマンド判定制御部
323　マスター鍵記憶部
323a　マスター鍵
323b　暗号化マスター鍵
324　特殊領域アクセス制御部
325　認証領域アクセス制御部
326　非認証領域アクセス制御部
327　暗号・復号化回路
331　非認証領域
332　認証領域
341　メディアID
342　製造メーカ名
343　セキュアメディアID
425　暗号化キー
426　暗号化コンテンツ
427　ユーザデータ
501　代替ブロック領域
812　読み出し回数
913　デジタル出力許可回数
1003　乱数発生器
1004　セクタ
1005　拡張領域
1006　ECCデータ
1007　時変領域
1101　変換テーブル
1102　認証領域専用変換テーブル
1103　非認証領域専用変換テーブル
1203　未消去リスト
1301　マスター鍵
1302　機器固有ID
1310　機器固有ID群記憶領域
1311　ユーザキー記憶領域

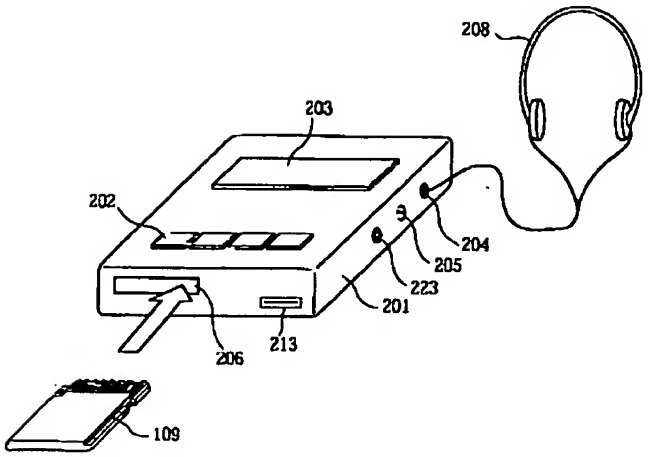
【図1】



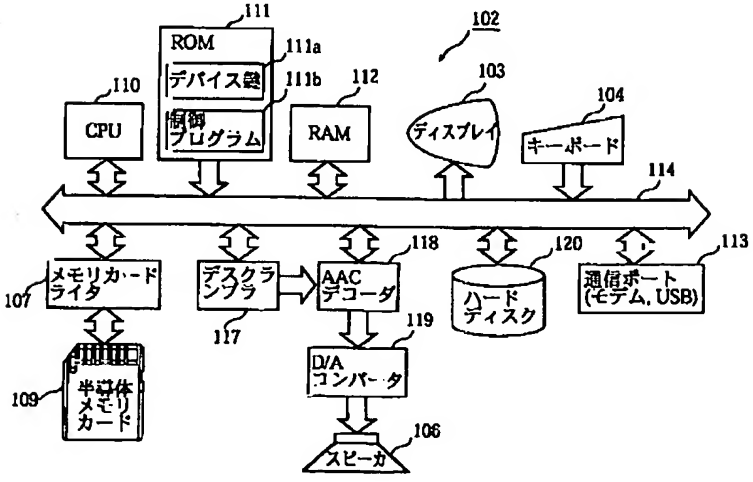
【図17】



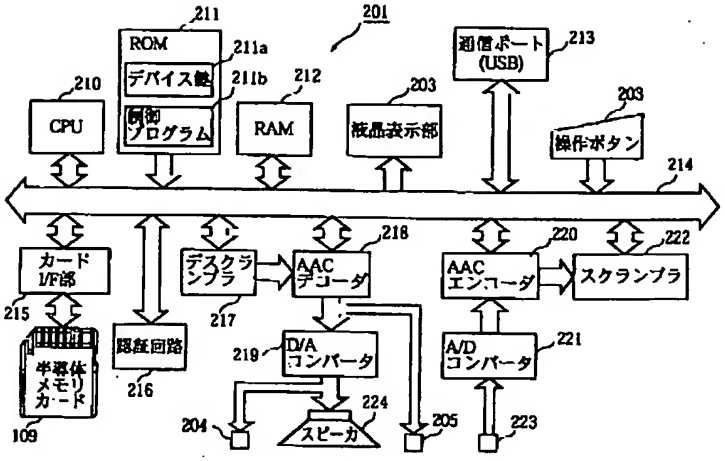
【図2】


208
203
202
204
205
223
201
206
213
109

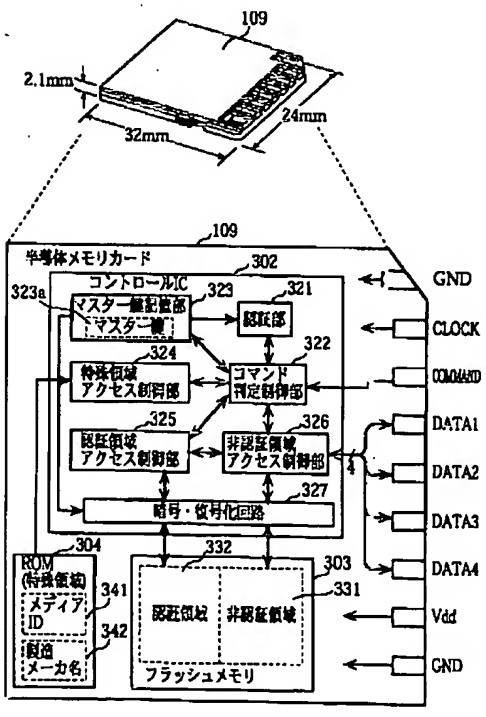
【図3】


111
ROM
111a
デバイス鍵
111b
制御プログラム
110
CPU
112
RAM
102
103
ディスプレイ
104
キーボード
114
107
メモリカードライタ
117
デスクランブラ
118
AACデコーダ
119
D/Aコンバータ
106
スピーカ
109
半導体メモリカード
120
ハードディスク
113
通信ポート(モデム, USB)

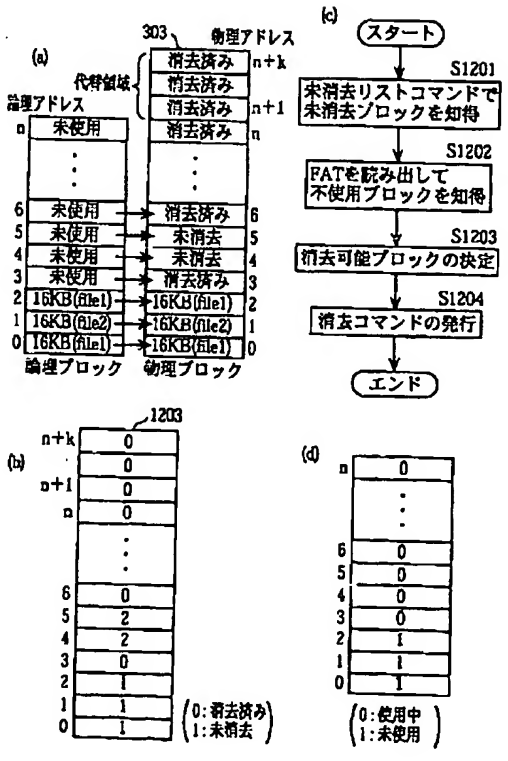
【図4】


211
ROM
211a
デバイス鍵
211b
制御プログラム
201
210
CPU
212
RAM
203
液晶表示部
通信ポート(USB)
213
203
操作ボタン
214
カードI/F部
215
半導体メモリカード
109
認証回路
216
デスクランブラ
217
218
AACデコーダ
D/Aコンバータ
219
220
AACエンコーダ
A/Dコンバータ
221
222
スクランブラ
224
スピーカ
204
205
223

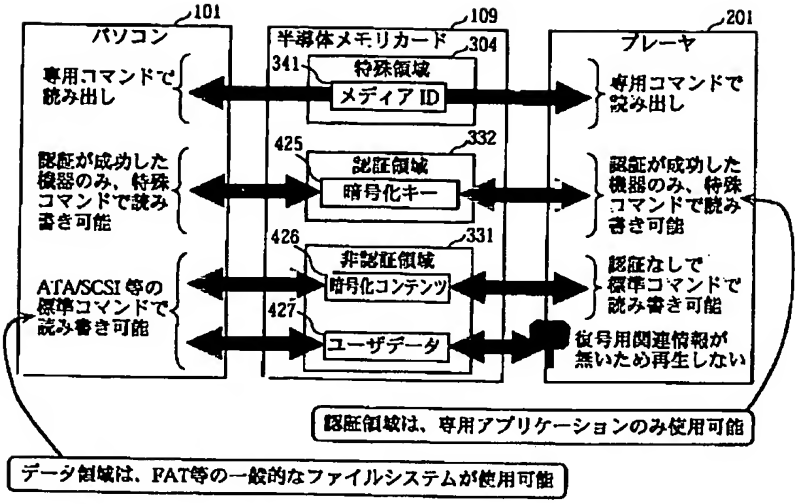
【図5】


109
2.1mm
32mm
24mm
半導体メモリカード
302
コントロールIC
323
321
323a
マスター鍵記憶部
マスター鍵
認証部
322
324
特殊領域アクセス制御部
コマンド判定制御部
325
326
認証領域アクセス制御部
非認証領域アクセス制御部
327
暗号・復号化回路
304
ROM(特殊領域)
341
メディアID
342
製造メーカ名
332
303
331
認証領域
非認証領域
フラッシュメモリ
GND
CLOCK
COMMAND
DATA1
DATA2
DATA3
DATA4
Vdd
GND

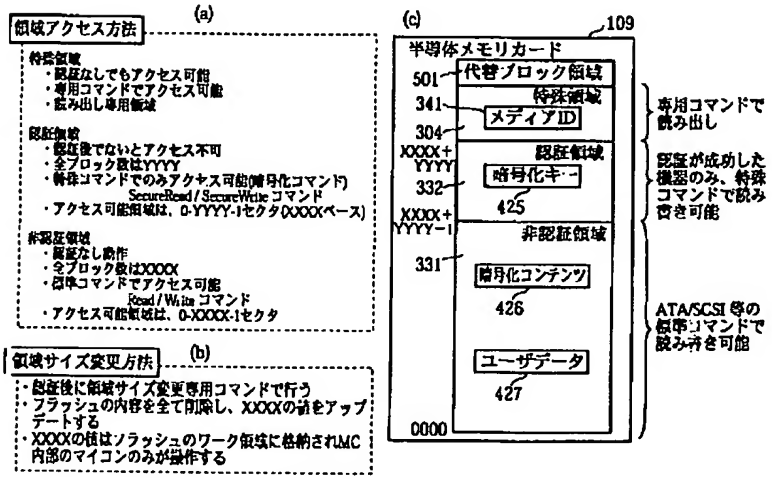
【図14】


(a)
303
物理アドレス
代替領域
論理アドレス
未使用
消去済み
未消去
16KB(file1)
16KB(file2)
論理ブロック
物理ブロック
(b)
1203
(0:消去済み
1:未消去)
(c)
スタート
S1201
未消去リストコマンドで未消去ブロックを知得
S1202
FATを読み出して不使用ブロックを知得
S1203
消去可能ブロックの決定
S1204
消去コマンドの発行
エンド
(d)
(0:使用中
1:未使用)

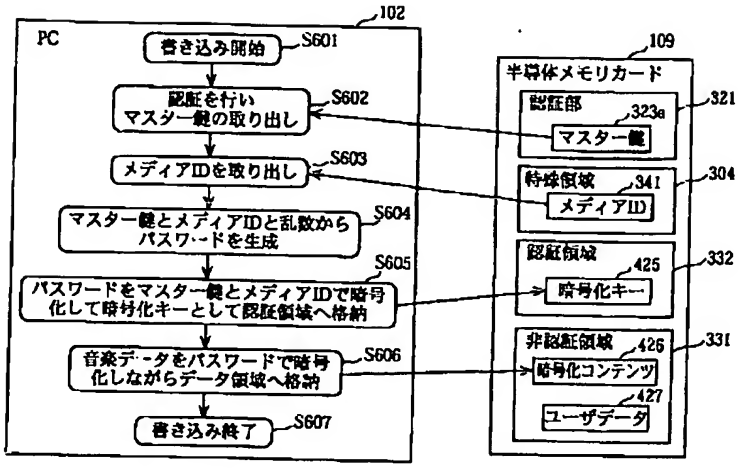
【図6】


101
パソコン
109
半導体メモリカード
304
201
プレーヤ
専用コマンドで読み出し
341
特殊領域
メディアID
専用コマンドで読み出し
認証が成功した機器のみ、特殊コマンドで読み書き可能
425
認証領域
332
暗号化キー
認証が成功した機器のみ、特殊コマンドで読み書き可能
ATA/SCSI等の標準コマンドで読み書き可能
426
非認証領域
331
暗号化コンテンツ
認証なしで標準コマンドで読み書き可能
427
ユーザデータ
復号用関連情報が無いため再生しない
認証領域は、専用アプリケーションのみ使用可能
データ領域は、FAT等の一般的なファイルシステムが使用可能

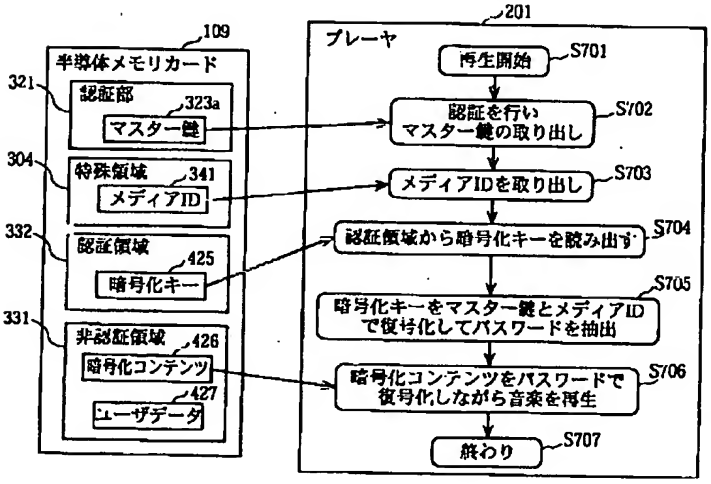
【図7】


領域アクセス方法
(a)
特殊領域
・認証なしでもアクセス可能
・専用コマンドでアクセス可能
・読み出し専用領域
認証領域
・認証後でないとアクセス不可
・全ブロック数はYYYY
・特殊コマンドでのみアクセス可能(暗号化コマンド)
SecureRead / SecureWrite コマンド
・アクセス可能領域は、0-YYYY-1セクタ(XXXXベース)
非認証領域
・認証なし動作
・全ブロック数はXXXX
・標準コマンドでアクセス可能
Read / Write コマンド
・アクセス可能領域は、0-XXXX-1セクタ
領域サイズ変更方法
(b)
・認証後に領域サイズ変更専用コマンドで行う
・フラッシュの内容を全て削除し、XXXXの値をアップデートする
・XXXXの値はフラッシュのワーク領域に格納されLMC内部のマイコンのみが操作する
(c)
109
半導体メモリカード
501
代替ブロック領域
特殊領域
341
メディアID
304
XXXX+YYYY
認証領域
332
暗号化キー
425
XXXX+YYYY-1
非認証領域
331
暗号化コンテンツ
426
ユーザデータ
427
0000
専用コマンドで読み出し
認証が成功した機器のみ、特殊コマンドで読み書き可能
ATA/SCSI等の標準コマンドで読み書き可能

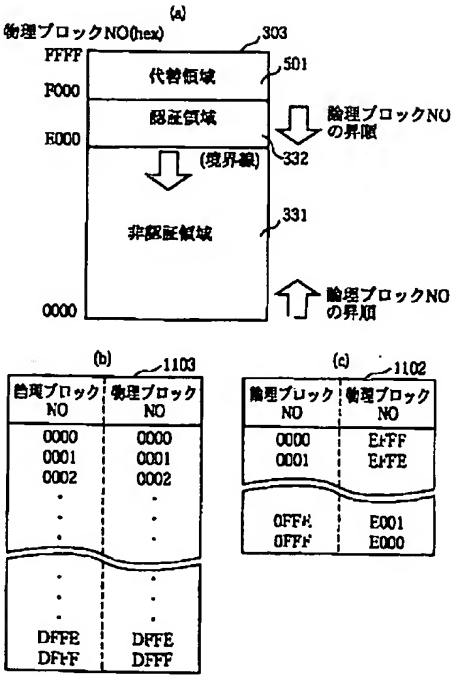
【図8】


102
PC
書き込み開始
S601
認証を行い
マスター鍵の取り出し
S602
メディアIDを取り出し
S603
マスター鍵とメディアIDと乱数から
パスワードを生成
S604
パスワードをマスター鍵とメディアIDで暗号
化して暗号化キーとして認証領域へ格納
S605
音楽データをパスワードで暗号
化しながらデータ領域へ格納
S606
書き込み終了
S607
109
半導体メモリカード
認証部
323a
マスター鍵
321
特殊領域
341
メディアID
304
認証領域
425
暗号化キー
332
非認証領域
426
暗号化コンテンツ
331
427
ユーザデータ

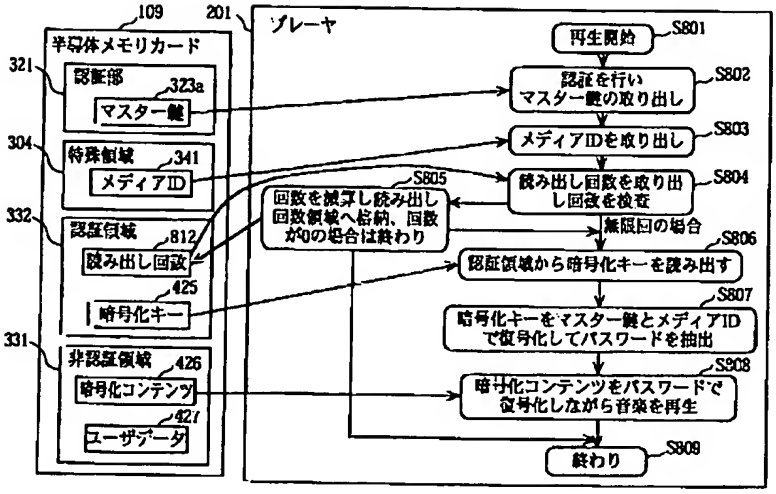
【図9】


201
プレーヤ
再生開始
S701
認証を行い
マスター鍵の取り出し
S702
メディアIDを取り出し
S703
認証領域から暗号化キーを読み出す
S704
暗号化キーをマスター鍵とメディアID
で復号化してパスワードを抽出
S705
暗号化コンテンツをパスワードで
復号化しながら音楽を再生
S706
終わり
S707
109
半導体メモリカード
321
認証部
323a
マスター鍵
304
特殊領域
341
メディアID
332
認証領域
425
暗号化キー
331
非認証領域
426
暗号化コンテンツ
427
ユーザデータ

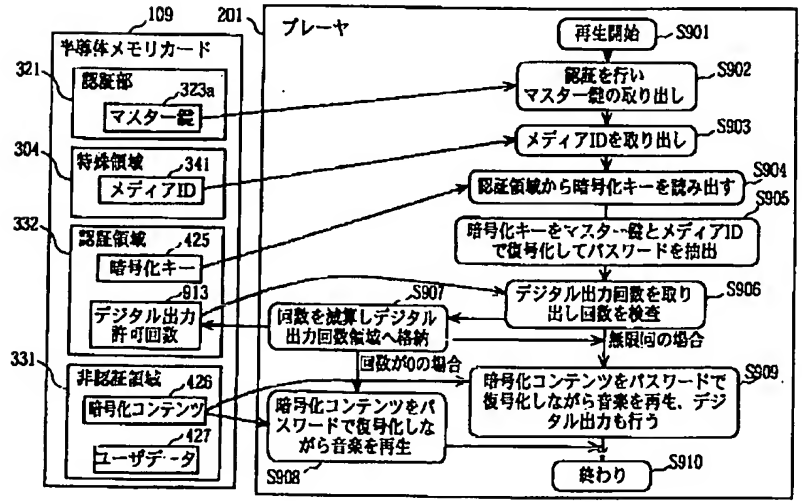
【図18】


(a)
物理ブロックNO(hex)
303
FFFF
F000
E000
0000
代替領域
501
認証領域
332
(境界線)
非認証領域
331
論理ブロックNO
の昇順
論理ブロックNO
の昇順
(b)
1103
論理ブロック
NO
物理ブロック
NO
0000
0001
0002
DFFE
DFFF
(c)
1102
論理ブロック
NO
物理ブロック
NO
0000
0001
EFFF
EFFE
OFFE
OFFF
E001
E000

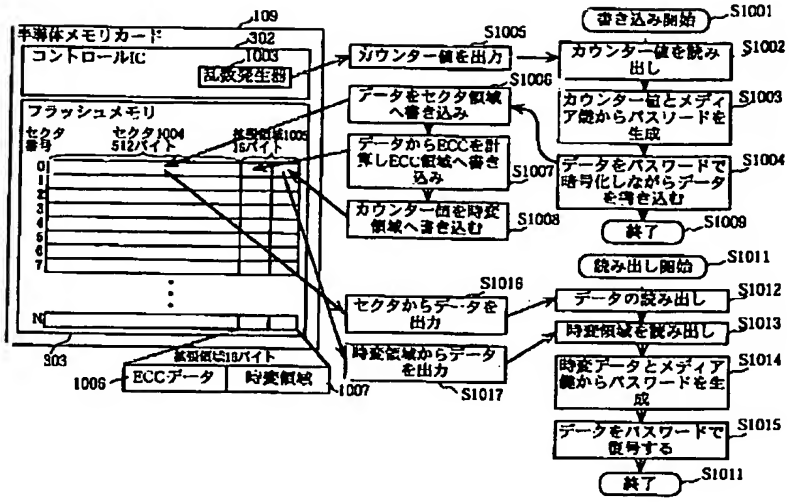
【図10】


109
201
半導体メモリカード
プレーヤ
321
認証部
323a
マスター鍵
304
特殊領域
341
メディアID
332
認証領域
812
読み出し回数
425
暗号化キー
331
非認証領域
426
暗号化コンテンツ
427
ユーザデータ
再生開始
S801
認証を行い
マスター鍵の取り出し
S802
メディアIDを取り出し
S803
読み出し回数を取り出し回数を検査
S804
回数を減算し読み出し回数領域へ格納、回数が0の場合は終わり
S805
無限回の場合
認証領域から暗号化キーを読み出す
S806
暗号化キーをマスター鍵とメディアIDで復号化してパスワードを抽出
S807
暗号化コンテンツをパスワードで復号化しながら音楽を再生
S808
終わり
S809

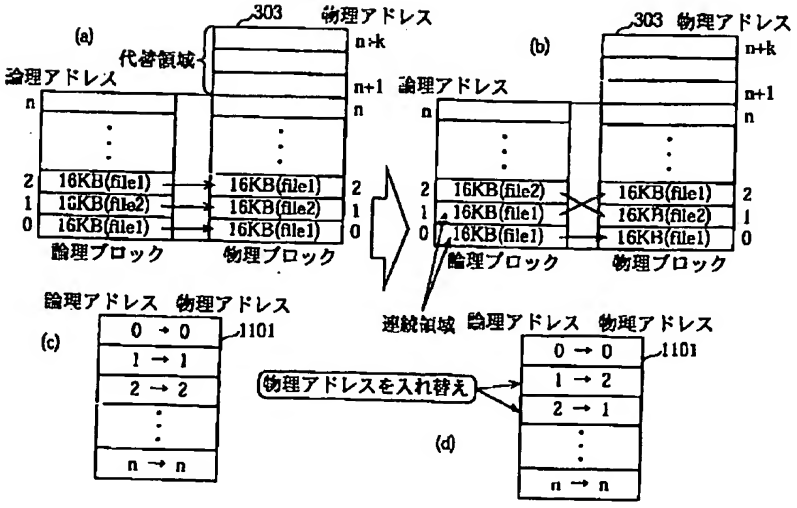
【図11】


109
201
半導体メモリカード
プレーヤ
321
認証部
323a
マスター鍵
304
特殊領域
341
メディアID
332
認証領域
425
暗号化キー
813
デジタル出力許可回数
331
非認証領域
426
暗号化コンテンツ
427
ユーザデータ
再生開始
S901
認証を行い
マスター鍵の取り出し
S902
メディアIDを取り出し
S903
認証領域から暗号化キーを読み出す
S904
暗号化キーをマスター鍵とメディアIDで復号化してパスワードを抽出
S905
デジタル出力回数を取り出し回数を検査
S906
回数を減算しデジタル出力回数領域へ格納
S907
無限回の場合
回数が0の場合
暗号化コンテンツをパスワードで復号化しながら音楽を再生、デジタル出力も行う
S909
暗号化コンテンツをパスワードで復号化しながら音楽を再生
S908
終わり
S910

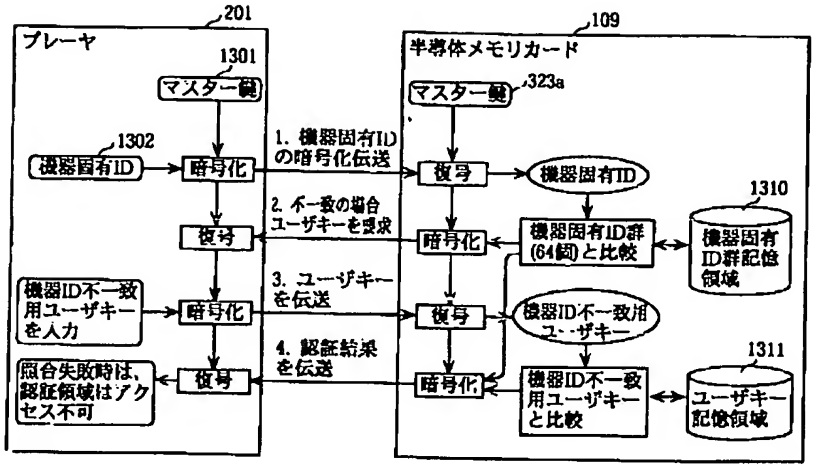
【図12】


半導体メモリカード
109
302
コントロールIC
1003
乱数発生器
フラッシュメモリ
セクタ番号
セクタ1004 512バイト
冗長領域1005 16バイト
303
ECCデータ
時変領域
1006
1007
カウンター値を出力
S1005
データをセクタ領域へ書き込み
S1006
データからECCを計算しECC領域へ書き込み
S1007
カウンター値を時変領域へ書き込む
S1008
書き込み開始
S1001
カウンター値を読み出し
S1002
カウンター値とメディア鍵からパスワードを生成
S1003
データをパスワードで暗号化しながらデータを書き込む
S1004
終了
S1009
読み出し開始
S1011
セクタからデータを出力
S1016
時変領域からデータを出力
S1017
データの読み出し
S1012
時変領域を読み出し
S1013
時変データとメディア鍵からパスワードを生成
S1014
データをパスワードで復号する
S1015
終了
S1011

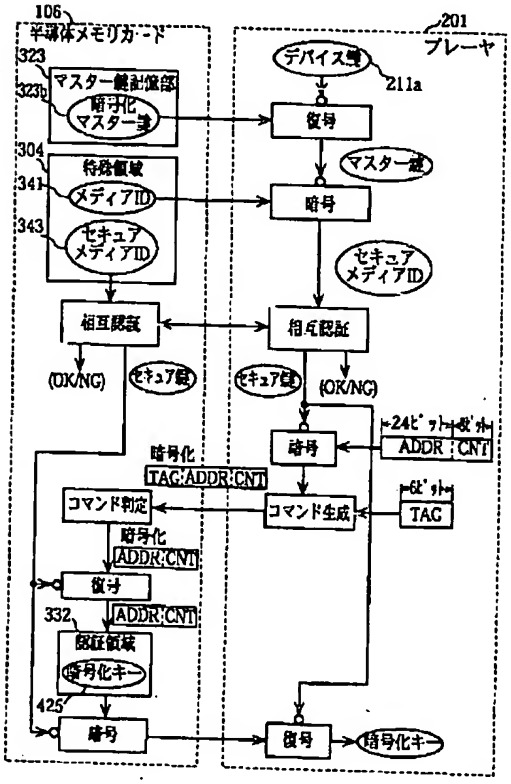
【図13】


(a)
303 物理アドレス
代替領域
論理アドレス
n+k
n+1
n
2 16KB(file1) 16KB(file1) 2
1 16KB(file2) 16KB(file2) 1
0 16KB(file1) 16KB(file1) 0
論理ブロック
物理ブロック
(b)
303 物理アドレス
論理アドレス
2 16KB(file2) 16KB(file1) 2
1 16KB(file1) 16KB(file2) 1
0 16KB(file1) 16KB(file1) 0
論理ブロック
物理ブロック
(c)
論理アドレス 物理アドレス
0 → 0
1 → 1
2 → 2
n → n
1101
連続領域
物理アドレスを入れ替え
(d)
論理アドレス 物理アドレス
0 → 0
1 → 2
2 → 1
n → n
1101

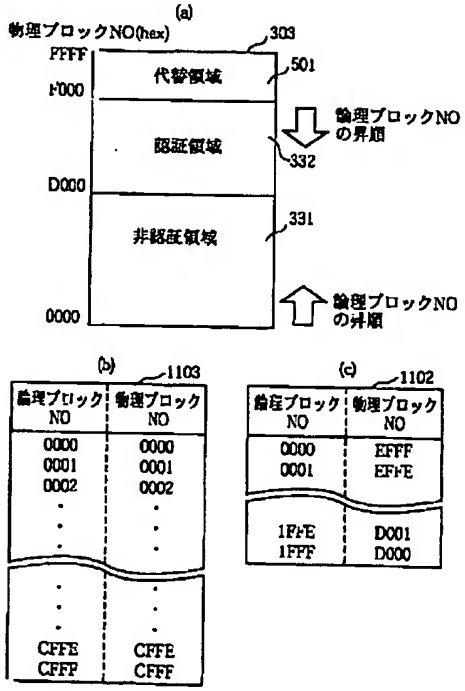
【図15】



【図16】



【図19】



フロントページの続き

(51)Int.Cl.⁷	識別記号	FI		(参考)
G09C 1/00	640	G09C 1/00	660A	
	660	G06K 19/00	R	

H04L 9/32

H04L 9/00 675A

(72)発明者 湯川 泰平
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72)発明者 南 賢尚
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72)発明者 小塚 雅之
大阪府門真市大字門真1006番地 松下電器産業株式会社内

Fターム(参考) 5B017 AA03 AA06 BA01 BA07 BB10 CA14
5B035 AA13 BB09 BB11 CA11 CA29
5B058 CA02 CA23 CA24 CA25 KA01 KA02 KA04 KA06 KA12 KA31 KA35
5J104 AA07 DA02 KA02 NA35